GENERAL INSURANCE COUNCIL

Insurance Regulatory and Development Authority (IRDA)

Business Continuity Plan for IIB

Insurance Information Bureau Project

Version 1.0

December, 2010

DOCUMENT RELEASE NOTICE

Notice No:
Client: IRDA
Project: Insurance Information Bureau
Revision History:

Date	Version	Description	Author
08-Dec-2010	V1.0	Initial Release	IIB Team

Distribution List:

Recipient	Location	Media
IIB ï Project Production Support Team	9th Floor, United India Insurance, Hyderabad	Electronic
IRDA Data Center	9th Floor, United India Insurance, Hyderabad	Electronic
General Insurance council (GIC)	Mumbai	Electronic

This document or revised pages are subject to document control.
Please keep them updated using the release notice from the distributor of the document.

Preface

Purpose

The purpose of this Business continuity plan and Disaster recovery document is to describe the configuration of failover and switch over aspects of the Insurance Information Bureau (IIB) Application.

This document also defines the Business continuity plan and Disaster recovery for the IIB.

Intended Audience

The intended audience for this security document is:

- IT team at IRDA
- TCS support team

Contents

List of Abbreviations

Abbreviation/ Acronym	Expansion
BCP	**Business Continuity PLAN**
IIB	**Insurance Information Bureau**
IRDA	**Insurance Regulatory and Development Authority**
RA	**Risk Assessment**
DBA	**Database Administrator**
ODG	**Oracle Data Guard**
ARO	**Asset Retirement Obligations**

1. INTRODUCTION

The outlines stipulated by the BCP enable the datacentre to effectively deal with disasters, which have the potential to disrupt the business and operations of the centre, thus ensuring continuity and recovery of the activities.

The BCP outlines:

- The contingency plans during business threatening emergencies,
- The plans to ensure continuity of business, and
- The path to complete recovery in the event of any loss, damage or failure of any of the facilities at the IIB datacentre.

1.1 Offsite Libraries

The tapes or other secondary storage media and vital records are Handover to IRDA.

1.2 Insurance

IRDA is Responsible for getting all the assets insured.

1.3 Backup and Restoration

Backup strategy anticipates failure at any step of the processing cycle and a mitigation plan is prepared as per requirement. Some of the measures taken under backup strategy are:

- A backup of the data is created every month.
- Master files are retained at appropriate intervals, such as the end of an updating procedure, to provide synchronisation between files and systems.
- An inventory of all offsite storage locations is maintained and it contains the following:
    - Tape Number (indicating daily or weekly backup),
    - Tape received on,
    - Tape sent on,
    - Current location, and
    - Destination of the tape.
- Data backup strategy for every system is recorded and contains atleast the following information: Frequency of the backup
- Backup medium (cartridge, disk)
- Day on which the backup is taken (i.e. backup schedule)

- Retention period and rotation cycle
- Verification procedures to ensure proper backup is taken
- Number of copies of the backup stored offsite and at the primary site.

The delivery centre at IRDA data centre was setup in 2010. The IRDA data centre has the capacity to accommodate 20 professionals; presently, it accommodates 15 professionals.

IIB is setup on the 9th floor of United India Towers, Basheerbagh, Hyderabad. It houses the best dedicated communication lines and cables which are used in global communication and provide excellent infrastructure facilities for IIB.

1.4 Primary Site – Basheerbagh , Hyderabad

The primary site at United India Towers, Basheerbagh, Hyderabad is connected with the help of a Cisco 2960 Series SI router. The workstations available in the IRDA datacenter are guarded by external firewalls and are connected to the router using Cisco Switch stack. The Cisco 2960 router is connected with its counterpart in the redundant site 1/ 2 using a 2 MBPS link.

1.5 Redundant Site 1

The redundant site1 at IRDA main office is located at Parshuram Bhavan, Basheerbaug, Hyderabad.

Note: IRDA is responsible for the site.

2. Risk Assessment

2.1 Overview

As a step towards building this Business Continuity Plan (BCP), a Risk Assessment (RA) was conducted to evaluate the effect of a disaster or outage on the business of the centre. Each functional area and process was evaluated to determine the financial and operational implications arising out of their unavailability. Thus RA served as the foundation for prioritising recovery of the various functional operations based on their criticality to business at IRDA datacenter.

RA related activities were discussed with individual support groups. This helped to capture the operational impacts of a disaster on the identified set of processes.

2.2 Methodology Adopted

The RA consists of the following steps:

1. Project Planning: This involved identifying the various process owners at IIB as the RA participants.

2. Data Collection: Data was primarily collected by TCS support group.
   (Appendix A contains the Infrastructure Data details and Appendix B contains the calculation for Disaster and ARO.)

3. Data Analysis: This involved identification of all the activities at the centre and the various threats that pose a risk to the continuity of business at the time of a disaster. The annualised rate of occurrence of each of these threats and the annualised loss expectancy for each activity under each threat was taken into account to plan the continuity strategy for the activities.

3. Failover Recovery

3.1 Parameter Settings:

The following table outlines various parameters for primary and standby databases:

Table 1: Parameter settings

Type of parameter setting	For primary database	For standby database
initBBP.ora parameters	**Data guard parameters for primary database:** *.db_name='IIBPROD' *.log_archive_dest_1='location=/oradata/IIBPROD/archive valid_for=(ALL_LOGFILES,ALL_ROLES) db_unique_name=IIBPROD' *.log_archive_dest_2='service=STANDBY LGWR ASYNC valid_for=(ONLINE_LOGFILES,PRIMARY_ROLE) db_unique_name=BackupDB' *.log_archive_dest_state_1='ENABLE' *.log_archive_dest_state_2='ENABLE' *.FAL_SERVER='STANDBY'	**Data guard parameters for standby database:** *.db_name='IIBPROD' *.log_archive_dest_1='location=/oradata/IIBPROD/archive VALID_FOR=(ALL_LOGFILES,ALL_ROLES) db_unique_name=BackupDB' *.log_archive_dest_2='service=PRIMARY LGWR ASYNC VALID_FOR=(ONLINE_LOGFILES,PRIMARY_ROLE) db_unique_name=IIBPROD' *.log_archive_dest_state_1=ENABLE *.log_archive_dest_state_2=DEFER FAL_SERVER=PRIMARY FAL_CLIENT=STANDBY *.standby_archive_dest='/oracle/BEP/oraarch' STANDBY_FILE_MANAGEMENT=AUTO *.SERVICE_NAMES=IIBPROD

	*.FAL_CLIENT='PRIMARY' *.standby_archive_dest='/oracle/BEP/oraarch/' *.STANDBY_FILE_MANAGEMENT='AUTO' *.service_names='BEP_STBY.WORLD'	
Oracle-net Service Configuration	**TNS name entries for primary database (tnsnames.ora):** ## # Filename.....: tnsnames.ora # Created.....: # Name.....: # Date.....: ## PRIMARY = (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(HOST = 192.168.0.201)(PORT = 1521))) (CONNECT_DATA = (SERVICE_NAME = IIBPROD))) STANDBY = (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(HOST = 192.168.0.203)(PORT = 1521))	**TNS names entries for standby (tnsnames.ora):** ## # Filename.....: tnsnames.ora # Created.....: # Name.....: # Date.....: ## PRIMARY = (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(HOST = 192.168.0.201)(PORT = 1521))) (CONNECT_DATA = (SERVICE_NAME = IIBPROD))) STANDBY = (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(HOST = 192.168.0.203)(PORT = 1521))) (CONNECT_DATA = (SERVICE_NAME = IIBPROD)))

	) (CONNECT_DATA = (SERVICE_NAME = IIBPROD)))	
Listener.ora Paramaters	**Listner.ora entries for primary database:** ## # Filename.....: listener.ora # Created.....: # Name.....: # Date.....: ## SID_LIST_LISTENER = (SID_LIST = (SID_DESC = (SID_NAME = PLSExtProc) (ORACLE_HOME = /u01/db/oracle/product/10.2.0/db_1) (PROGRAM = extproc)) (SID_DESC = (SID_NAME = IIBPROD) (ORACLE_HOME = /u01/db/oracle/product/10.2.0/db_1))) LISTENER = (DESCRIPTION_LIST = (DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)(HOST = IIBDB)(PORT = 1521))))	**Listner.ora entries for Standby:** ## # Filename.....: listener.ora # Created.....: # Name.....: # Date.....: ## SID_LIST_LISTENER = (SID_LIST = (SID_DESC = (SID_NAME = PLSExtProc) (ORACLE_HOME = /u01/db/oracle/product/10.2.0/db_1) (PROGRAM = extproc)) (SID_DESC = (SID_NAME = IIBPROD) (ORACLE_HOME = /u01/db/oracle/product/10.2.0/db_1))) LISTENER = (DESCRIPTION_LIST = (DESCRIPTION = (ADDRESS = (PROTOCOL = TCP)(HOST = BackupDB)(PORT = 1521))))

Sqlnet.ora for primary and standby databases	**Sqlnet.ora** should be same for both primary and standby instances Sqlnet.ora ## # Filename.....: sqlnet.ora # Created.....: # Name.....: # Date.....: ## PRIMARY VALUES NAMES.DIRECTORY_PATH= (TNSNAMES, LDAP, EZCONNECT) STANDBY VALUES NAMES.DIRECTORY_PATH= (TNSNAMES, EZCONNECT, LDAP)	

4. Application Failover

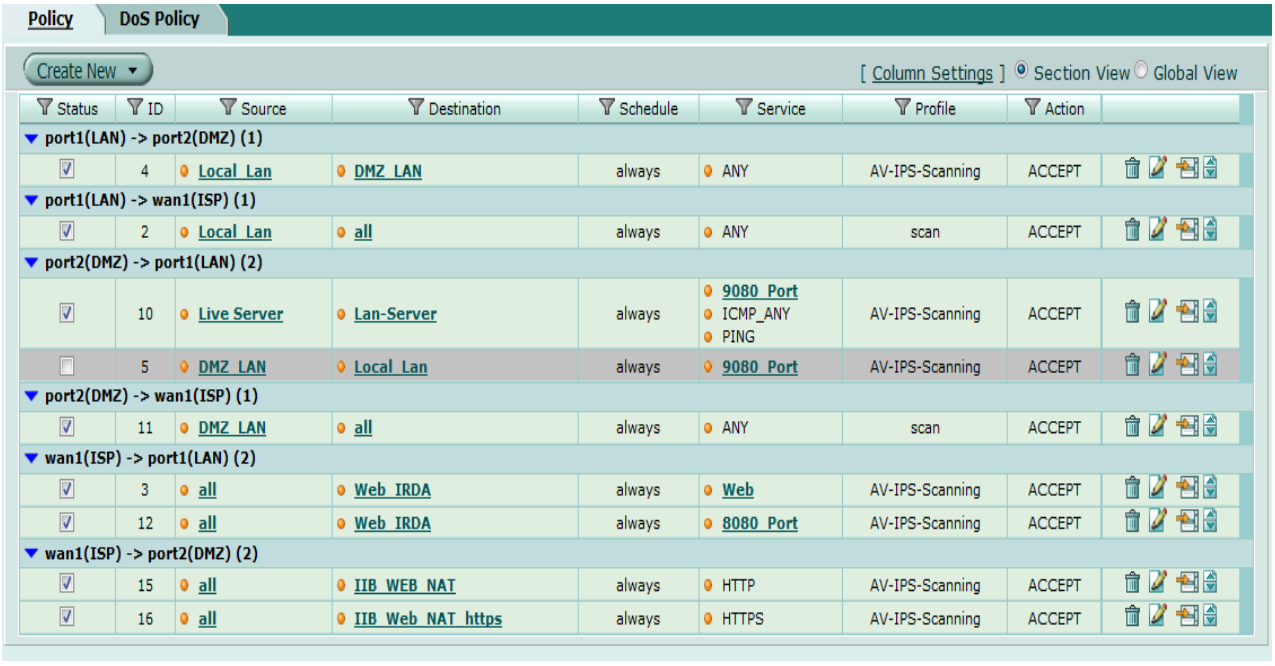
4.1 Web server Configuration:

Primary webserver will have the communication to the primary point to the application server and secondary point to the standby application server.
If primary Appserver is not reachable or not responded then request is routed to the standby appserver.
Both webservers have the same configuration.
Note: if any one of webserver or appserver fails then automatically standby(Failover) server will respond for the request that is both are active- active.

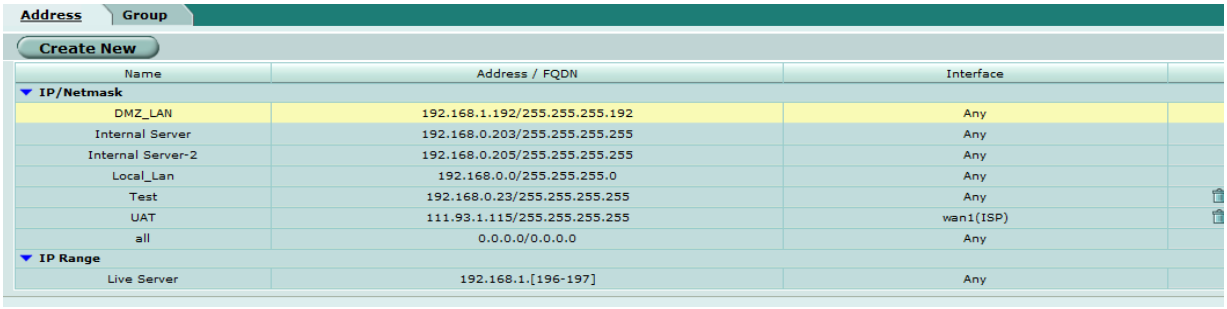
Firewall has configured the load balanced for the web servers if primary web server does not respond then request will redirect to the secondary web server and vice versa.

Following are the configuration done on Fortigate Firewall.

4.2 IRDA Firewall Policies



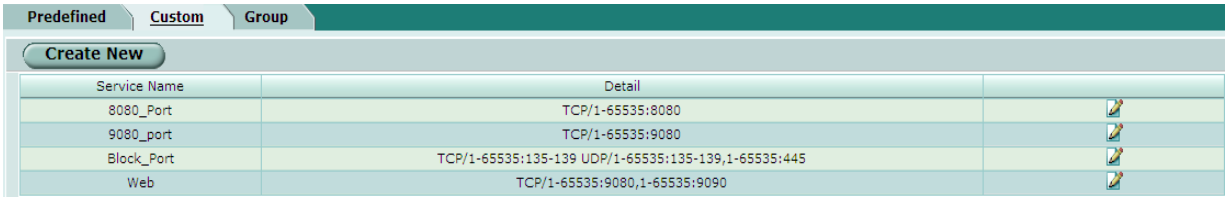
4.3 IPADDRESS:



4.4 Services:

Firewall services define one or more protocols and port numbers associated with each service. Service definitions are used by firewall policies to match session types. You can organize related services into service groups to simplify your firewall Policy list.

Defined services are follows.

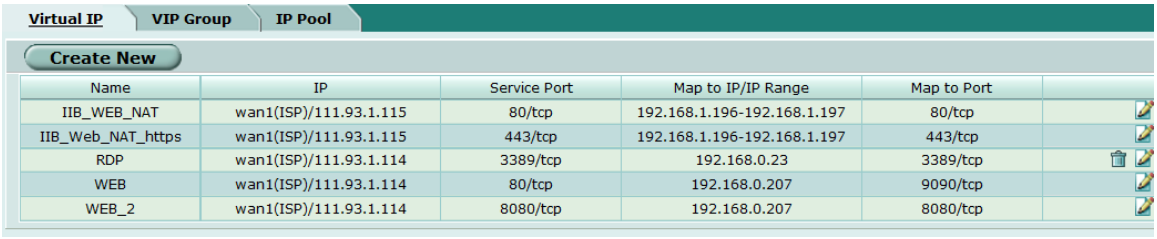


4.5 Virtual IP:

Virtual IP addresses (VIPs) can be used when configuring firewall policies to translate IP addresses and ports of packets received by a network interface, including a modem interface.

When the FortiGate unit receives inbound packets matching a firewall policy whose Destination Address field is a virtual IP, the FortiGate unit applies NAT, replacing packetsôIP addresses with the virtual IPôs mapped IP address.

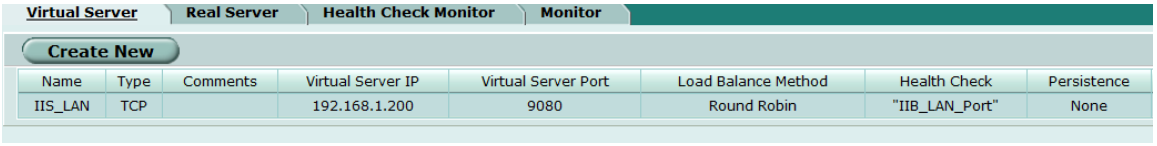
Here We have PAT the internal mail server IP for access the application from the outside (WAN).



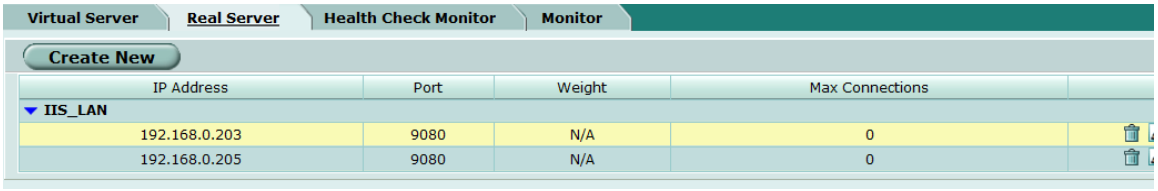
Name	IP	Service Port	Map to IP/IP Range	Map to Port
IIB_WEB_NAT	wan1(ISP)/111.93.1.115	80/tcp	192.168.1.196-192.168.1.197	80/tcp
IIB_Web_NAT_https	wan1(ISP)/111.93.1.115	443/tcp	192.168.1.196-192.168.1.197	443/tcp
RDP	wan1(ISP)/111.93.1.114	3389/tcp	192.168.0.23	3389/tcp
WEB	wan1(ISP)/111.93.1.114	80/tcp	192.168.0.207	9090/tcp
WEB_2	wan1(ISP)/111.93.1.114	8080/tcp	192.168.0.207	8080/tcp

4.6 Virtual Server:

We are Defining Virtual Server for load balancing of WEB Server on Round Robin Load Balancing Method.



Name	Type	Comments	Virtual Server IP	Virtual Server Port	Load Balance Method	Health Check	Persistence
IIS_LAN	TCP		192.168.1.200	9080	Round Robin	"IIB_LAN_Port"	None

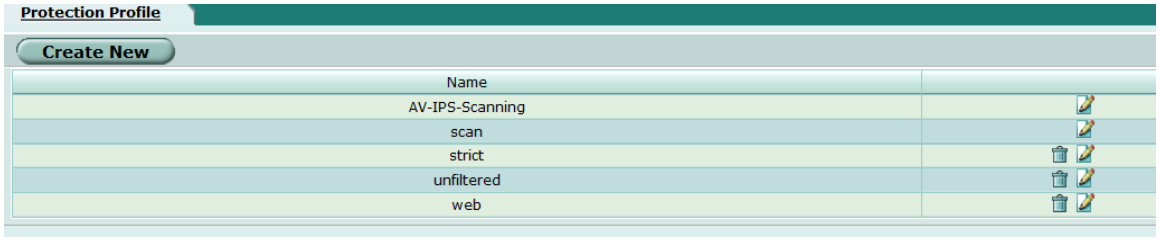


IP Address	Port	Weight	Max Connections
IIS_LAN			
192.168.0.203	9080	N/A	0
192.168.0.205	9080	N/A	0

4.7 Protection Profile:

A protection profile is a group of settings that you can apply to one or more firewall policies. Because protection profiles can be used by more than one firewall policy, you can configure once a protection profile for the traffic types handled by a set of firewall policies requiring identical protection levels and types, rather than repeatedly configuring those same protection profile settings for each individual firewall policy.

You can use protection profiles to configure:
ÅAntivirus protection
ÅWeb filtering
ÅFortiGuard Web Filtering
ÅSpam filtering
ÅIPS
ÅContent archiving



We are enable AV Scanning as well as IPS in ñ**AV-IPS Scanning Protection**òprofile & it attached the policy No :- 3 / 12 / 15 /16 / 4 / 5 accessing the Nated IP through WAN to Lan/DMZ

We are enable AV Scanning as well as IPS in ñ**SCAN** ñProtection profile & it attached the policy No :- 2 /11 for accessing the Internet through Lan To WAN

5. Business Continuity and Disaster Recovery

IRDA has to subscribe with third party vendor for same set of environment.

TCS will take incremental cold backup on tape drive every week and hand it over to the IRDA. IRDA/TCS has to perform the DR Drill on an ongoing basis.

5.1 Project Management

Responsibility

The responsibility of managing in case of any disaster will be with the IRDA Data center Team.

Action List

1. Identify the incident responsible for hampering network management activity
2. Arrange a meeting with Emergency Management Team (IS, Admin, Transport teams of IRDA, GL/PL of the Project) to discuss restoration strategy based on the following inputs:
   - Network link(s) availability by consulting with the service provider.
   - Availability of hardware and spare components in the inventory to support certain key activities.
3. Depending on the gravity of the disaster and the extent of damage to the assets:
   - Prepare resource requirements checklist based on the recovery strategy.
   - Retrieve the list of hardware inventories at the offsite storage location and perform the gap analysis
   - Place orders with vendors for additional requirements.
   - Retrieve the following vital records from their records pertaining to IS operations:
     i. Minimum hardware and software configuration lists for all systems
     ii. Network procedure manual containing detail procedures to set up networking components like routers, switches.
     iii. Backup and restoration procedures for all systems
     - Set up the LAN infrastructure
     - Set up the WAN infrastructure
     - Setup User desktops

When the environment is ready, it will take 3 days to resume normal availability of the application.

As the proposed sites work in Active ï Passive mode, application failover approach is as given below:

- **Declaration of Disaster** : This is a process in itself and activities for the same needs to be defined
- **Network Switchover :** On declaration of Disaster,
  - All traffic to DC will be stopped
  - The network switchover solution will enable the user to reach the DR site instead of DC
- **Storage Switchover:** The continuous data replication will reduce the data loss and improve upon the RPO.

- **Server Switchover:** As a policy and regular update mechanism at DR site, all the servers will have the same O/S versions, patches, and shall have the same application environment with all patches/ updates/ upgrades as at DC. This synchronization will be done on regular periodicity.
- **Database Startup at DR**: The DR database will be started and the replicated database images will be mounted and restored.
- **Application Startup at DR :** This will require:
    - All the Application instances and application scripts will be activated *available*
    - Application scripts will be verified.
    - A DR Plan willdefine the Phase wise resumption of the application keeping the data integrity intact
    - All the service will be tested for functioning and will be resumed
    - Monitor the Services for specified/Agreed period in DR Plan to watch for any irregular activity/ non-available services/ any other issues.
- **Testing:** Testing of all the application running properly and delivering results in normal mode will be conducted and once the switchover is successful ï DR Site will be declared operational.

6. Appendix

6.1 Appendix A Software Hardware list Table

Hardware List

SNo.	Workload	Description	Qty
1	Web server	x3550M2 with 1 x Intel 5504 4C 2.0GHz, 8GB RAM, 2 x 146GB HDD	2
3	Application server	x3550M2 with 1 x Intel 5504 4C 2.0GHz, 8GB RAM, 2 x 146GB HDD	1
4	Database server	x3550M2 with 1 x Intel 5502 2C 1.86GHz, 16GB RAM, 2 x 146GB HDD, 2 x FC HBA	1
5	App/DB failover and Backup/Mgt Server	x3550M2 with 1 x Intel 5504 4C 2.0 GHz, 16GB RAM, 2 x 146GB HDD, 2 x FC HBA	1
6	Test & Dev Server	x3550M2 with 2 x Intel 5502 2C 1.86GHz, 8GB RAM, 2 x146GB HDD	1
7	Storage	2TB usable RAID5 - DS3400 2GB cache with 9 x 300GB SAS	1
8	SAN switch	CISCO MDS 9124 with 8 ports active	1
9	Tape Backup	TS3200 with 48 slots and 2 x FC attach LTO4 drives and path failover license	1
10	Hypervisor	VMWare eSXi Hardware	1

Software List

SNo.	Workload	Description	Qty
1	Application Server	IBM WEBSPHERE APPLICATION SERVER NETWORK DEPLOYMENT PROCESSOR VALUE UNIT (PVU) LICENSE + SW SUBSCRIPTION & SUPPORT	1
3	Web server	IBM HTTP Server	2
4	Database Server	Oracle 10g Enterprise Edition	1CPU (Production) + 25 NUP (Test/Dev)
5	Database Server Options	Oracle Partitioning	1CPU (Production) + 25 NUP (Test/Dev)2
6	Operating System	Redhat Enterprise License Advanced Platform	6

SNo.	Workload	Description	Qty
7	Data Quality	DataClean™	1
8	Encryption	SSL Certificates	2
9	Backup Management	IBM TIVOLI STORAGE MANAGER EXTENDED EDITION	1
10	Backup Management	IBM TIVOLI STORAGE MANAGER FOR DATABASES	1
11	Backup Management	IBM TIVOLI STORAGE MANAGER STORAGE AREA NETWORKS	1

6.2 Appendix B Disaster and ARO Calculation Table

Srl. No.	Type of Disaster	Relocation Required	Data Collected	ARO
1	Flash Floods	Yes	No incident so far	0
2	Tsunami	Yes	No incident so far	0
3	War	Yes	5 incidents of war in 55 years.	0.09
4	Terrorism	Yes	There are lot of terrorism but No attack on commercial building so far	0
5	Earthquakes	Yes		0
6	Cyclonic storms	Yes	No incident so far	0
7	Theft	No	No incident so far	0
8	Sabotage	Yes	No incident so far	0
9	Fire outbreaks	Yes	No incident so far	0
10	Power outages	Yes		
11	Network components failure	No		0
12	Intrusions	No	No incident so far	0
13	Virus Attacks	No		0
14	Human Error In Processing	No	No incident so far	0
15	System Crashes	No		0
16	Communication Link Failure	Yes		0
17	Civil Strife	Yes	No incident so far	0

6.3 Appendix C Assets with approx. cost table

Srl.No.	Asset at the centre	Approx. Cost of asset (in Lakhs)
1.	Webserver Server	
2.	Switches	
3.	Routers	
4.	Desktops	
5.	UPS	
6.	Application server	

7.	Database Server	
8.	Printers	
9.	Communication Link	
10.	Firewall	
11.	Telephones	

7. Glossary

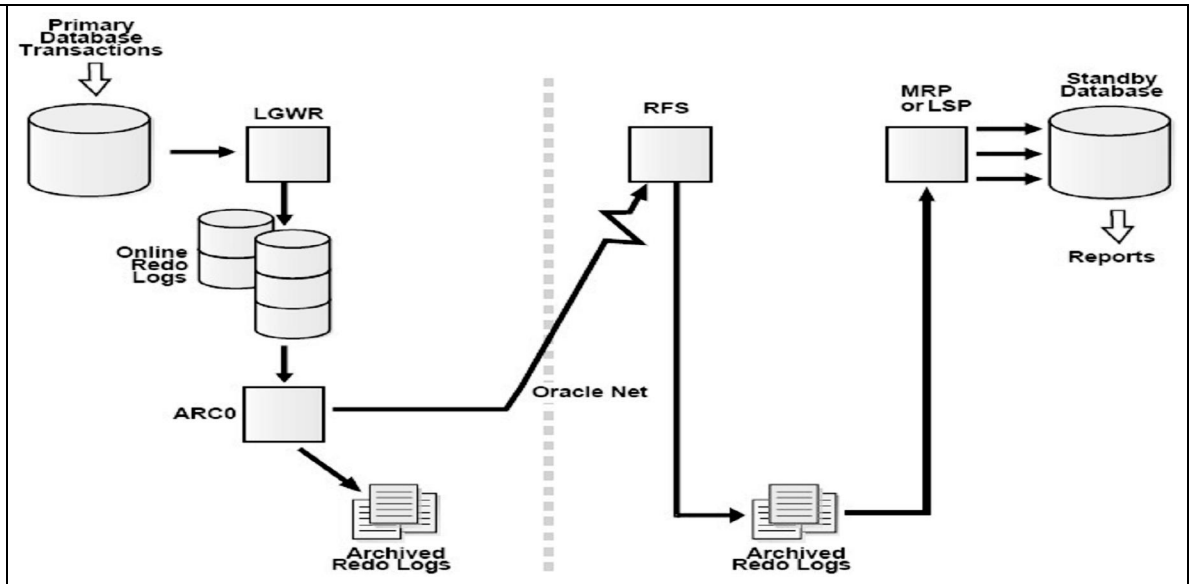
D	Data Guard	ñAn application-transparent high-performance low-impact asymmetrical online reliable Redo or SQL level background standby database transaction exchange utility capable of reporting, switchover and Failover.ò Data Guard helps us to protect data. It takes the data from the Production Server and automatically puts it in another location (Standby Database) and makes it available for Switchover and Failover operations.
	Data Guard Configuration	A Data Guard Configuration (DGC) consists of one production database and one or more standby databases. The databases in a DGC are connected by Oracle Net and may be dispersed geographically. There are no restrictions on where the databases are located, provided they can communicate with each other. For example, you can have a standby database on the same system as the production database, along with two standby databases on other systems at remote locations. You can manage primary and standby databases using the SQL command-line interfaces or the data guard broker interfaces, including a command-line interface (DGMGRL) and a graphical user interface that is integrated in Oracle Enterprise Manager.
O	Oracle Data Guard	ODG ensures high availability, data protection, and disaster recovery for enterprise data. ODG provides a comprehensive set of services that create, maintain, manage, and monitor one or more standby databases to enable production Oracle databases to survive disasters and data corruptions. It maintains these standby databases as transitionally consistent copies of the production database. Then, if the production database becomes unavailable because of a planned or an unplanned outage, Data Guard can switch any standby database to the production role, minimizing the downtime associated with the outage. ODG can be used with traditional backup, restoration, and cluster techniques to provide a high level of data protection and data availability. With ODG, administrators can optionally improve production database performance by offloading resource-intensive backup and reporting operations to standby systems.

<table>
<tr><td>P</td><td>Primary Database</td><td>A DGC contains one production database, also referred to as the primary database that functions in the primary role. This is the database that is accessed by most of our applications. The primary database can be either a single-instance Oracle database or an Oracle Real Application Clusters database.</td></tr>
<tr><td>S</td><td>Standby Database</td><td>A standby database is a transitionally consistent copy of the primary database. Using a backup copy of the primary database, you can create up to nine standby databases and incorporate them in a DGC. Once created, Data Guard automatically maintains each standby database by transmitting redo data from the primary database and then applying the redo to the standby database. Similar to a primary database, a standby database can be either a single-instance Oracle database or an Oracle Real Application Clusters database.

A standby database can be of two types:

Table 2:Types of Standby databases
<table>
<tr><td>S. no.</td><td>Category</td><td>Physical Standby database</td><td>Logical Standby database</td></tr>
<tr><td>1.</td><td>Definition</td><td>Physical Standby database provides a physically identical copy of the primary database with disk database structures that are identical to the primary database structures. The database schemas, including indexes, are the same.</td><td>Logical standby database contains the same logical information as the production database, although the physical organization and structure of the data can be different.</td></tr>
<tr><td>2.</td><td>Synchronization</td><td>A physical standby database is kept synchronized with the primary database, though</td><td>The logical standby database is kept synchronized with the primary database through SQL Apply, which transforms the data in the redo</td></tr>
</table>
</td></tr>
</table>

				Redo Apply, which recovers the redo data, received from the primary database and applies redo to the physical standby database.	received from the primary database into SQL statements and then executing the SQL statements on the standby database.
		3.	Application	A physical standby database can be used for business purposes other than disaster recovery, on a limited basis.	A logical standby database can be used for other business purposes in addition to disaster recovery requirements. Also, using a logical standby database, you can upgrade Oracle Database software and patch sets with almost no downtime. Thus, a logical standby database can be used concurrently for data protection, reporting, and database upgrades.
T	Technical Diagram	**The following figure illustrates transmitting and applying archived Redo logs to a Physical Standby Database**			


Primary Database Transactions
LGWR
Online Redo Logs
ARC0
Archived Redo Logs
Oracle Net
RFS
Archived Redo Logs
MRP or LSP
Standby Database
Reports