The Oriental Insurance Company Limited

Head Office, New Delhi

Request for Proposal

For

Technology Refresh for DC and DR Infrastructure

(Ref No: OICL/HO/ITD/TECH-REFRESH/2015/01 dated 28th August 2015)

Information Technology Department

The Oriental Insurance Company Limited

2nd Floor, Oriental House

A-25/27, Asaf Ali Road, New Delhi – 110 002

CIN-U66010DL1947GOI007158

www.orientalinsurance.org.in

This page is

Intentionally

Left blank

(Non – Transferable)
Receipt

Tender No. OICL/HO/ITD/ TECH-REFRESH/2015/01 Dated 28th August 2015

Serial No: _____

Date of Issue: ____ / ____ /_____

Tender Form Issued To

_____

_____

Received Payment Vide Demand Draft / Pay Order No _____

Dated ____/____/_____ for _____/- issued by

_____ (BANK).

Signature: _____

Name: _____

Designation: _____

This page is

Intentionally

Left blank

(Non – Transferable)
Receipt

Tender No. OICL/HO/ITD/ TECH-REFRESH/2015/01 Dated 28th August 2015

Serial No: _____

Date of Issue: ____ / ____ /_____

Tender Form Issued To

_____

_____

Received Payment Vide Demand Draft / Pay Order No _____

Dated ____/____/_____ **for** _____/- **issued by**

_____ **(BANK).**

Signature: _____

Name: _____

Designation: _____

This page is

Intentionally

Left blank

Important Notice

This document is the property of The Oriental Insurance Company Ltd (OICL). It should not be copied, distributed or recorded on any medium (electronic or otherwise) without OICL's written permission. Use of contents given in this document, even by the authorised personnel/agencies for any purpose other than that specified herein, is strictly prohibited as it shall amount to copyright violation and thus shall be punishable under the Indian law.

This tender document is not transferable.

Bidders are advised to study this tender document carefully. Submission of bid shall be deemed to have been done after careful study and examination of the tender document with full understanding of its implications.

The response to this tender should be full and complete in all respects. Incomplete or partial bids shall be rejected. The Bidder must quote for all the items asked for, in this tender.

The Bidder shall bear all costs associated with the preparation and submission of the bid, including cost of presentation and demonstration for the purposes of clarification of the bid, if so desired by OICL. OICL will in no case be responsible or liable for those costs, regardless of the conduct or outcome of the bidding process.

Table of Contents

1. Introduction 13
1.1 About the Company 13
1.2 Notice Inviting Bids 13
1.3 Project Objective 13
1.4 Schedule of Events 14
1.5 Availability of tender document 14
1.6 Eligibility Criteria 15
1.7 Project Timelines 17
2. Background & Current Infrastructure 18
2.1 Existing Inventory – Bengaluru 18
2.2 Existing Inventory – Vashi (Navi Mumbai) 20
3. Summary of Requirements 22
4. Scope of Work 23
4.1 General 23
4.2 Storage 24
4.2.1. Existing Storage Details 24
4.2.2. Scope of Work for Storage 25
4.3 Servers 26
4.4 Network & Security 26
4.5 Backup Solution 27
4.6 DR Management Solution 29
4.7 Mail Messaging Solution 29
4.8 Bulk (Volume) Mail 30
4.9 Proxy Server/ Appliance 30
4.10 Support during Warranty & AMC Period 30
4.11 AMC of Existing Oracle T4 Servers 32
4.12 Migration 32
4.13 Facility Management Services 33
4.13.1. Services to be Implemented by Bidder at DC and DR Site 33
4.13.2. 24 x 7 Onsite Support 35
4.13.3. Advanced Monitoring and Reporting Services 38
4.14 Project Management 39
4.15 Documentation 40
4.15.1. Documentation along with Technical Bid 40
4.15.2. Documentation & Reports Post Award of PO 40
4.16 Shifting of Hardware from one location to another 42
5. Terms & Conditions 43
5.1 General 43
5.1.1 Definitions 43
5.1.2 Amendment to Bid Document 43

5.1.3 Acceptance of the Solution 44
5.1.4 Sub-contracts 44
5.1.5 Conditional bids 44
5.1.6 Submission of Bids 45
5.1.7 Performance Security 45
5.1.8 Pre-Bid Meeting 45
5.1.9 Installation and Implementation 45
5.1.10 Delay in Bidder's performance 45
5.1.11 Payment terms 46
5.1.12 Mode of Payment 47
5.1.13 Currency of Payments 47
5.2 Other RFP Requirements 47
6. Terms of Reference ('ToR') 48
6.1 Contract Commitment 48
6.2 Ownership, Grant and Delivery 48
6.3 Completeness of Project 48
6.4 Assignment 48
6.5 Canvassing/Contacting 48
6.6 Indemnity 48
6.7 Inspection of Records 49
6.8 Publicity 49
6.9 Solicitation of Employees 49
6.10 Information Ownership 49
6.11 Sensitive Information 49
6.12 Confidentiality 50
6.13 Technological Advancements 50
6.14 Liquidated Damages 50
6.15 Guarantees 51
6.16 Termination for Default 51
6.17 Force Majeure 51
6.18 Termination for Insolvency 51
6.19 Termination for Convenience 52
6.20 Resolution of disputes 52
6.21 Governing Language 52
6.22 Applicable Law 52
6.23 Prices 53
6.24 Taxes & Duties 53
6.25 Deduction 53
6.26 No Claim Certificate 53
6.27 Rights reserved by OICL 53
6.28 Limitation of Liability 53

6.29 Waiver 53
6.30 Violation of terms 54
6.31 Repeat Order 54
7. Service Level Agreement 55
8. Instruction to Bidders 58
8.1 Procedure for submission of Bids 58
8.2 Bid Security 59
9. Bid Documents 60
9.1 Eligibility Bid Documents 60
9.2 Technical Bid Documents 60
9.3 Commercial Bid Documents 61
10. Evaluation Process 62
10.1 Eligibility Evaluation 62
10.2 Technical Evaluation 62
10.3 Commercial Evaluation 62
11. Disclaimer 63
12. Appendix 64
12.1 Appendix 1: Bill of Material 65
12.2 Appendix 2 : Covering Technical Offer 74
12.3 Appendix 3 : Query Format 75
12.4 Appendix 4 : Summary of Documents Submitted 76
4.1 – Eligibility Bid Compliance 76
4.2 – Technical Bid Compliance 76
12.5 Appendix 5 : Pro forma for Bid Security 77
12.6 Appendix 6 : Pro forma for Performance Security 78
12.7 Appendix 7 : OEM's Authorization Form 79
12.8 Appendix 8 : Statement of No Deviation from Tender Terms and Conditions 80
13. Annexures 81
13.1 Annexure 1 : Technical Specifications 82
13.1.1 Enterprise Storage System 82
13.1.2 SAN Switch 84
13.1.3 FC-IP Routers 85
13.1.4 Tape Library 86
13.1.5 Disk Based Backup Appliance 87
13.1.6 Backup Software 88
13.1.7 Blade Chassis 90
13.1.8 Backup Server 91
13.1.9 NOC & HRMS Reporting Servers 92
13.1.10 Mail Messaging Servers 93
13.1.11 DR Management and Other Servers 94
13.1.12 Server - CTA 95

13.1.13 Server - OEM 96
13.1.14 Core Switch 97
13.1.15 DMZ Switch 101
13.1.16 Distribution Switch 105
13.1.17 Core & DMZ Firewall with Integrated IPS 109
13.1.18 Server Load Balancer 113
13.1.19 Application Delivery Controller 115
13.1.20 42U Rack 118
13.1.21 IP Based KVM Switch 118
13.1.22 Mail Messaging Solution 119
13.1.23 Proxy Server Solution 128
13.1.24 DR Management Software 130
13.1.25 Desktop 131
13.2 Annexure 2 : Evaluation Methodology 132
13.3 Annexure 3 : Authorization letter to attend tender opening 135
13.4 Annexure 4 : Details of Similar Projects Undertaken in last 5 Years 136
13.5 Annexure 5 : Application form for Eligibility Bid 137
13.6 Annexure 6 : Contract Form 139
13.7 Annexure 7 : List of Buy-Back Equipment 141
13.8 Annexure 8: Hardware Sizing for Mail Messaging Solution 150
13.9 Annexure 9: Power Details for Proposed Hardware 151
13.10 Annexure 10: Proposed DC-DR Layout 152
13.11 Annexure 11: Application Framework 153

Purpose of this document

The purpose of this Request for Proposal (hereafter referred to as "RFP") is to define the scope of work for the Bidder for OICL's Technology Refresh for DC and DR Infrastructure.

This RFP contains details regarding the scope, project timelines, evaluation process, terms and conditions as well as other relevant details which the Bidder needs to factor in while responding to this RFP.

Definitions and Acronyms

Following terms are used in the document interchangeably to mean:

AMC	Annual Maintenance Contract
ATR	Acceptance Test Report
ATS	Annual Technical Support
Bidder	Single point appointed by OICL for procurement and supply of the solution, based on the bill of materials shared by OICL.
DC	Data Centre which is located at Bengaluru
DRS/DRC/DR	Disaster Recovery Site which is located in Mumbai
EMD	Earnest Money Deposit
INR	Indian Rupees
LAN	Local Area Network
MPLS	Multi-Protocol Label Switching
NCR	National Capital Region
OEM	Original Equipment Manufacturer
OICL	Oriental Insurance Company Limited
PO	Purchase Order
RFP	Request for Proposal
SOW	Scope of Work
T&C	Terms & Conditions
TCO	Total Cost of Ownership
ToR	Terms of Reference
UAT	User Acceptance Test

1. Introduction

1.1 About the Company

The Oriental Insurance Company Limited (OICL), a public sector undertaking dealing in non-life insurance, is ahead of its peers in the industry in adopting information technology. OICL has been enjoying the highest rating from leading Indian credit rating agencies such as CRISIL and ICRA.

OICL has its head office at New Delhi, Primary Data Centre (PDC) at Bengaluru & Secondary Data Centre (SDC/DR) at Vashi (Navi Mumbai), 30 regional offices in various cities, Oriental Staff Training Colleges (OSTC) at Faridabad and Chennai, 340+ divisional offices, 500+ branch offices, Regional Training Centers, 28 Claims Service centers, 32 TP Hubs and 900+ extension counters/micro offices geographically spread out across India. Currently the head office has 5 buildings located in New Delhi along with OSTC Faridabad.

As on date, all offices of OICL are provisioned with dual active-active links using MPLS over RF, leased lines etc. Further, Roam connectivity is provided to EC's and Micro Offices. For more than a decade, OICL has leveraged information technology to serve its customers effectively. The company also has a presence in Nepal, Dubai and Kuwait.

Apart from the Core-Insurance application (INLIAS), OICL has various centralized applications like web portal, E-mail, Video Conferencing, HRMS etc. hosted at its Data Centers at Vashi and Bengaluru. These Data Centers are equipped with Rack Mounted Servers, Blade Servers, Enterprise Class Storage systems, Tape Libraries, SAN Switches, Backup Solution and other related tools and solutions.

The company has sold more than 12 million new policies in the year 2014-15.The Company has more than 100 general insurance products to cater to the varied insurance needs of its customers. It also has a strong workforce of about 15,000 employees and over 35,000 agents. The Company has a web portal www.orientalinsurance.org.in for use of its customers and agents with a provision for premium calculator, payment gateway and online issue/ renewal of policies.

1.2 Notice Inviting Bids

The Deputy General Manager (IT) invites sealed bids from eligible Bidders for Technology Refresh for DC & DR Infrastructure and to undertake Facilities Management of the Infrastructure for the tenure of the contract.

1.3 Project Objective

The Oriental Insurance Company Ltd (OICL) envisages refreshing the end of life IT Infrastructure and implementing new technology solutions to meet its business and technology requirements. OICL proposes to invite sealed bids from eligible companies for Supply, Installation, Implementation, Migration and Support of IT Infrastructure Solutions to be deployed at Data Centre and Disaster Recovery Site for a period of six years.

OICL has its Data centre at Bengaluru and Disaster Recovery Site at Vashi (Navi Mumbai). OICL intends to identify new co-hosting space for data centre and disaster recovery site within the same cities through a separate RFP process. Bidder shall also be responsible for seamless migration of the existing infrastructure from the old DC and DR sites to the new DC and DR sites.

1.4 Schedule of Events

Event	Target Date
Sale of RFP Document	28th August 2015 to 16th October 2015
Last date to send in requests for clarifications	4th September 2015; 5:00 PM
Pre-Bid meeting	11th September 2015, 2:00 PM
Last date for submission of bids	**16th October 2015, 3:00 PM**
Opening of pre-qualification bid	16th October 2015, 3:15 PM
Declaration of Short-listing of Bidders based on pre-qualification criteria	Shall be announced later
Opening of technical bid	Shall be announced later
Technical Presentation	Shall be announced later
Declaration of short-list of Bidders for commercial bid	Shall be announced later
Opening of commercial bids	Shall be announced later
Declaration of L1 Bidder	Shall be announced later
Notification of Award	Shall be announced later

Note:

1. It is mandatory for the Bidder to purchase the tender document so as to participate in the pre-bid meeting.
2. OICL reserves the exclusive right to make any amendments / changes to or cancel any of the above actions or any other action related to this RFP.
3. If any of the above dates is declared a holiday for OICL, the next working date will be considered. OICL reserves the right to change the dates mentioned in the RFP.

1.5 Availability of tender document

a) This is a non–transferable RFP document containing conditions of pre-qualification, detailed requirement specifications as also the terms and conditions can be obtained from the address given below:

The Oriental Insurance Company Limited
Information Technology Department,
A - 25/27, 'Oriental House', 2nd Floor,
Asaf Ali Road, New Delhi – 110 002

b) The RFP document will be available for sale at the above address between 11.00 Hours to 16.00 Hours on all working days from 28th August 2015 to 16th October 2015 on payment of non-refundable Tender Fee of Rs. 5,000/- (Rupees Five thousands) by crossed Demand Draft/ Banker's Pay Order in favour of "The Oriental Insurance Company Limited" payable at New Delhi. Tender fee is inclusive of all taxes.

c) A Copy of the Tender document is available on the web portal www.orientalinsurance.org.in under the link 'Tenders'. Bidders have to purchase Tender document in order to submit bids. Please note that the Company shall not accept any liability for non-receipt/non-delivery of bid document(s) in time.

1.6 Eligibility Criteria

Bidders should meet the following eligibility criteria in order to bid for the RFP:

S.N.	Eligibility Criteria	Documents Required
General and Financial Criteria		
1	Should be a public / private limited company registered in India.	Certificate of Incorporation
2	The Bidder should have been in existence for a minimum period of FIVE years in India.	Certificate of Incorporation
3	The Bidder should have a minimum turnover of Rs.200 crores per annum in any three of the following financial years (2011-12, 2012-13, 2013-14, and 2014-15).	Audited Financial statements for the respective financial years and/or Published Balance Sheet
4	The Bidder should have a positive net worth in any three of the following financial years (2011-12, 2012-13, 2013-14, and 2014-15).	
5	The Bidder should have at least one of the following accreditations / certifications which is valid as on the date of issue of this RFP: ISO 9001:2008, ISO 27001, SEI CMMi Level 3.	Copy of relevant certifications
6	The Bidder should not have been blacklisted by the any Government or PSU enterprise.	Self-Declaration letter by Bidder authorized signatory duly authorized by the Board
7	The Bidder should hold a valid Sales Tax Registration/VAT/Service tax Certificate, PAN Card and should be registered with the appropriate authorities for all applicable statutory taxes/duties.	a. Attested copy of the Sales Tax Registration /VAT/Service tax certificate. b. Attested copy of PAN Card and Sales Registration number
8	The Bidder must provide support/service in the concerned activity at Mumbai and Bengaluru.	Self-Declaration by authorized signatory with following details: a. Location details and number of years it has been in existence. b. Contact details: Phone and Email of the person heading the Center.
Technical Eligibility Criteria		
1	The Bidder should have executed atleast two System Integration Projects involving delivery, installation and maintenance of IT Solutions like Servers, Storage, Backup, Network Switch, Firewall, Application Delivery Controller, Server Load Balancer, DR Management Tool, Mail Messaging in Government/ PSU/ BFSI sector in India in the last 5 years. (Value of each project should be more than INR 10 Crores and should consist of atleast 3 IT Infrastructure components mentioned above.)	
2	The Bidder should have executed project for delivery, installation and maintenance of Enterprise Storage in Government/ PSU/ BFSI sector in India in the last 5 years.	
3	The Bidder should have executed project for delivery, installation and maintenance of Backup Solution (Tape Library / Backup Software / Disk based solution) in Government/ PSU/ BFSI sector in India in the last 5 years.	
4	The Bidder should have executed project for delivery, installation and maintenance of Core Network Switches in Government/ PSU/ BFSI sector in India in the last 5 years.	
5	The Bidder should have executed project for delivery, installation and maintenance of Core Firewalls in Government/ PSU/ BFSI sector in India in the last 5 years.	

6	The Bidder should have executed project for delivery, installation and maintenance of Mail Messaging Solution in Government/ PSU/ BFSI sector in India in the last 5 years.
7	The Bidder shall have successfully provided Support or Maintenance Services (FMS) in Government/ PSU/ BFSI sector in India in the last 5 years.

Documents Required for each Technical Eligibility Criteria:

1. Copy of original PO / Contract highlighting the following details:
   a. Date of PO/ Contract
   b. Name of Parties
   c. Scope of Work
2. Completion Certificate or Installation Report or Satisfactory Progress of project from client.

1.7 Project Timelines

1.7.1 The Delivery, Migration, Configuration, Installation & Commissioning of all Hardware and Software shall be completed within a period of 24 Weeks from the date of placement of order.

Milestone	Milestones	Weeks from date of issue of Purchase Order
1	Purchase Order from OICL to successful Bidder	Week-0
2	System Study and finalization of Deployment architecture	Week-4
3	Submission of Project Plan detailing each task with target date and assigned resource persons including the plan for migration of existing infrastructure from Old DC to New DC and installation of all supplied items and integration with existing infrastructure at DC and DR Sites.	Week-8
4	Delivery of Hardware at New DC and DR Site	Week-10
5	Power-on, Basic Installation and configuration of all supplied items at DC and DR Sites.	Week-12
6	Completion of all work at the DC and DR Sites including migration and Integration of all equipment and implementation of Mail Messaging and DR Solution.	Week-22
7	Successful DR drill and documentation	Week-24

1.7.2 The delay in implementation will attract Liquidated Damages as per terms & conditions.

Note:

a) OICL, at its discretion, shall have the right to alter the delivery schedule and quantities based on the implementation plan. This will be communicated formally to the Bidder during the implementation, if a need arises.

b) The Bidder is required to provide a detailed strategy to OICL; the activities mentioned above are indicative but the timelines for procurement and delivery should be maintained. Hence if the Bidder has a faster and more effective solution the same may be discussed and agreed by OICL.

2. Background & Current Infrastructure

OICL is ahead of its peers in the industry in adopting information technology. The Oriental Insurance Company Ltd (OICL) has its Data Centre Site at Bengaluru and Disaster Recovery Site at Vashi (Navi Mumbai).

To bring uniformity, security and centralized access OICL has adopted an integrated non-life insurance application software, named INLIAS, with the help of a technology partner, M/s 3i-Infotech. The INLIAS application serves a majority of business requirements of OICL. Its scope covers underwriting, accounting, claims processing, report generation and reinsurance requirements. OICL is also using Oracle PeopleSoft HRMS solution for their employees. Currently these two applications are running on the Solaris Platform on Oracle Hardware at DC and DR Sites. OICL is in the process of migrating and consolidating these two applications in the latest Solaris Platform through a separate RFP process.

The Company also has a state-of-the-art web portal through which customers can transact, make payments and track the status of various transactions. The portal has login facilities for retail customers, employees, corporate brokers and agents.

OICL is currently using Sun Communication Express E-Mail Messaging Solution for their employees. OICL has various other centralized applications like Desktop Management Suite, Video Conferencing, SAP Investment management, etc. hosted at its Data Centers at Bengaluru and Vashi. OICL is also in process of implementing Enterprise Content Management Solution through a separate RFP process.

The following sections describe the existing inventory available at the DC and DR sites:

2.1 Existing Inventory – Bengaluru

S.N.	Model	Make	Qty	Purpose	Year of Purchase	Reuse/ Buyback	Shifting (Yes/No)
Servers							
1	T5120	Sun	1	Mail MTA (DR)	2009	Buyback	No
2	T5120	Sun	1	On-site T&D	2009	Buyback	No
3	T2000	Sun	1	Not in Use	2007	Buyback	No
4	T2000	Sun	1	Proxy BNG	2007	Buyback	No
5	V480	Sun	1	Oracle Enterprise server	2005	Buyback	No
6	M4000	Sun	1	Backup Server (DC)	2009	Buyback	No
7	SB6000 Blade Chassis	Sun	1	Blade Chassis	2009	Buyback	No
8	X6250 Blade	Sun	1	HRMS Reports (DC)	2009	Buyback	No
9	X6250 Blade	Sun	1	HRMS T&D	2009	Buyback	No
10	X6250 Blade	Sun	1	Antivirus Server (DR)	2009	Buyback	No
11	X6250 Blade	Sun	1	SSP-DC-Mgmt	2009	Buyback	No
12	X6250 Blade	Sun	5	SAP SERVER (DC)	2010	Buyback	No
13	HCL Server	HCL	3	Not in Use	2006	Buyback	No
14	SB6000 Blade Chassis	Sun	1	Blade Chassis	2011	Buyback	No
15	SB X6270 M2 Blade	Sun	1	3i Infotech Web Services (DC)	2011	Buyback	No
16	SB SPARC T3 Blade	Sun	1	HRMS Reporting Layer	2011	Buyback	No
17	x4150	Sun	1	NET ADMIN	2009	Buyback	No
18	UCS 5108 Blade Chassis	Cisco	2	Blade Chassis	2014	Reuse	Yes

19	UCS B200 M3 Blade Servers	Cisco	9	SAP (DC)	2014	Reuse	Yes
19	UCS B200 M3 Blade Servers	Cisco	7	EMS/AD/AV (DR)	2014	Reuse	Yes
20	HP c7000 Blade Chassis	HP	1	Blade Chassis	2015	Reuse	Yes
21	HP BL460 Blade Server	HP	16	Web Portal (DC)	2015	Reuse	Yes
Storage & Backup							
22	ST9990V	Sun	1	Sun-Storage	2009	Buyback	No
23	SL500	Sun	1	Tape Library	2009	Buyback	No
24	Brocade5100	Brocade	2	FC Switch	2009	Buyback	No
25	Brocade 7500	Brocade	2	FCIP Router	2009	Buyback	No
26	VMAX 20 K	EMC	1	100 TB Storage	2013	Reuse	Yes
27	Brocade DS 5300	Brocade	2	SAN Switch	2013	Reuse	Yes
28	HP DL 360 Gen8	HP	1	Management Server	2013	Reuse	Yes
Video Conferencing							
29	Polycom-RMX2000	Polycom	1	Video Conferencing	2011	Reuse	Yes
30	Polycom-CMA4000	Polycom	1	Video Conferencing	2011	Reuse	Yes
31	Polycom -UBP200E	Polycom	1	Video Conferencing	2011	Reuse	Yes
Desktops							
32	HP PC	PC	1	Solomon App Server	2004	Buyback	No
33	PC-1	SUN PC	5	Onsite team	2009	Buyback	No
34	Wipro Net	Wipro	1	HRMS Data Capturing	2010	Buyback	No
35	Wipro Desktop	Wipro	1	ESRS + Antivirus	2013	Reuse	Yes
Network & Security							
36	CISCO 6500-E	Cisco	2	Core Switch	2009	Buyback	No
37	CISCO ASA 5580	Cisco	2	Firewall	2009	Buyback	No
38	CISCO CATALYST 3750 G	Cisco	2	DMZ Switch	2009	Buyback	No
39	Cisco IPS 4260	Cisco	2	IPS	2009	Buyback	No
40	CISCO CATALYST 2950G	Cisco	1	L2 SWITCH	2009	Buyback	No
41	CISCO ACE 4710	Cisco	2	Load Balancer	2009	Buyback	No
42	Cisco ASR1002	Cisco	2	Core WAN Router	2012	Reuse	Yes
43	Cisco ASR1002	Cisco	2	IPSec Router	2012	Reuse	Yes
44	Cisco ASR1002	Cisco	2	Replication Router	2012	Reuse	Yes

2.2 Existing Inventory – Vashi (Navi Mumbai)

S.N.	Model	Make	Qty	Purpose	Year of Purchase	Reuse/ Buyback	Shifting (Yes/No)
Servers							
1	Sun-V490	Sun	1	Backup server (DR)	2007	Buyback	No
2	SUN-V480-02	Sun	1	INLIAS Reporting	2004	Buyback	No
3	SUN-E2900	Sun	1	INLIAS Reporting	2004	Buyback	No
4	SUN E2900-02	Sun	1	INLIAS Reporting	2004	Buyback	No
5	SE T5220	Sun	2	Mail server (DC)	2009	Buyback	No
6	SUN-V480-03	Sun	1	Proxy server	2004	Buyback	No
7	HCL 2700 CA	HCL	1	Trend Micro Control	2007	Buyback	No
8	Sun Fire X4170 M2	Sun	1	CTA Server	2007	Buyback	No
9	SUN-T5120	Sun	1	Web Portal server (DC)	2009	Buyback	No
10	Sunblade6000 Chassis	Sun	1	Web Portal chassis	2009	Buyback	No
11	SBT6320 Blade	Sun	7	Web Portal server Blade (DC)	2009	Buyback	No
12	HCL 2700 BD-2	HCL	1	HCL helpdesk server	2007	Buyback	No
13	Blade Chassis	HP	1	PC NOC	2004	Buyback	No
14	Blade Server	HP	6	PC NOC (DC)	2004	Buyback	No
15	HP DL580	HP	1	PC NOC (DC)	2004	Buyback	No
16	Infiniti Global Line 2700ST	HCL	4	NOC server 1	2007	Buyback	No
17	Infiniti Global Line 2700 XDN	HCL	1	SSP server	2007	Buyback	No
18	HP ML 110	HP	1	FTP Server	2007	Buyback	No
19	UCS 5108 Blade Chassis	Cisco	2	Blade Chassis	2014	Reuse	Yes
20a	UCS B200 M3 Servers	Cisco	2	SAP (DR)	2014	Reuse	Yes
20b	UCS B200 M3 Servers	Cisco	14	EMS, SAP, AV (DC)	2014	Reuse	Yes
21	HP c7000 Blade Chassis	HP	1	Blade Chassis	2015	Reuse	Yes
22	HP BL460 Blade Server	HP	10	Web Portal (DR)	2015	Reuse	Yes
Storage & Backup							
23	Silkworm 4100	Brocade	2	SAN switch	2004	Buyback	No
24	SUN-SL500	Sun	1	Tape Library	2007	Buyback	No
25	Sun Tape Drive	Sun	2	DDS-4 tape drive	2004	Buyback	No
26	SUN – L100	Sun	1	TAPE Library	2004	Buyback	No
27	half height LTO-3	Quantum	1	External Tape Drive	2004	Buyback	No
28	BrocadeSW7500	Brocade	2	FCIP Replication Router	2007	Buyback	No
29	EMC Clarrion Ax4-5	EMC	1	SAN Storage	2011	Reuse	Yes
30	Brocade DS 5300B	Brocade	2	EMC SAN Switch	2013	Reuse	Yes
31	EMC VMAX 20K	EMC	1	SAN storage	2012	Reuse	Yes
32	ESRS System	EMC	1	Console PC(EMC)	2012	Reuse	Yes
Network & Security							
33	CISCO-PIX 515 E	Cisco	2	DMZ Firewall	2004	Buyback	No
34	Cisco 3750	Cisco	2	DMZ switch	2004	Buyback	No
35	Cisco 6506	Cisco	2	Core switch	2004	Buyback	No

36	Cisco 2950	Cisco	2	Management switch	2004	Buyback	No
37	KVM switch		1	8 Ports KVM switch	2007	Buyback	No
38	HCL-24TMS-2GCS	HCL	1	24 port switch	2007	Buyback	No
39	SUN-E2900	SUN	3	NOT IN USE	2004	Buyback	No
40	Cisco AS 4710	Cisco	2	SLB	2012	Buyback	No
41	Cisco ASA 5585	Cisco	2	CORE FIREWALL	2012	Buyback	No
42	Cisco MCS 7800	Cisco	2	Call Manager	2004	Buyback	No
43	Cisco ASR1002	Cisco	2	Core WAN Router	2012	Reuse	Yes
44	Cisco ASR1002	Cisco	2	IPSec Router	2012	Reuse	Yes
45	Cisco ASR1002	Cisco	2	Replication Router	2012	Reuse	Yes
Desktops							
46	Sun 150	SUN	1	Workstation	2004	Buyback	No
47	HCL MONITOR	HCL	1	Console PC	2007	Buyback	No
48	HP MONITOR-5500	HP	1	Monitor	2005	Buyback	No
49	MONITOR	Compaq	1	Monitor	2005	Buyback	No

3. Summary of Requirements

OICL has a DC Site at Bengaluru and a DR Site at Vashi (Navi Mumbai) both hosted at Sify Data Centers. OICL has floated a separate RFP for new DC and DR Co-Hosting Space within the same cities i.e. Bengaluru and Mumbai/Navi Mumbai respectively. The Bidder shall be responsible for Supply, Installation, Implementation, Migration and Support of IT Infrastructure Solutions to be deployed at the two sites for a period of six years. The Bidder shall be responsible for seamless migration of Infrastructure from the existing sites to the new sites. The Bidders scope summary is as follows:

S.N.	Heads	Scope of Work – Summary
A	Storage	• The Bidder is required to supply, implement and maintain a new Storage Solution for DC & DR meeting the requirements of OICL during the tenure of the contract as per Minimum Technical Specifications mentioned in Annexure-1. • OICL will continue to use the existing Enterprise Storage present in OICL at DC & DR Site. Bidder has to migrate the data from existing storage systems to new storage.
B	Backup Solution	• The Bidder is required to supply, implement and maintain the backup solution i.e. Tape Library, Backup Software and Disk based appliance at DC & DR sites.
C	Networks & Security Infrastructure	• The Bidder is required to supply, implement and maintain the network & security infrastructure at DC & DR sites. • The Bidder shall be responsible for seamless migration from the existing data centers to new the data centers.
D	Automated DR Management Tool	• To implement and maintain the DR management tool to accommodate business and technology requirements of OICL.
E	Email	• Currently OICL has Sun Communication Express for Email solution. OICL is envisaging replacing the existing email solution. The Bidder is required to design, size, supply, implement and maintain enterprise email solution for 18000 users. • The bidder shall also provide DR Solution and Archival Solution. • The bidder shall also supply, configure and maintain Separate Bulk (Volume) Mail Solution
F	Servers	• Design, size, supply, implement and maintain the new servers along with OS required for Mail Messaging, Backup and other required solution as part of this RFP.
G	Proxy Solution	• The bidder shall implement and maintain internet proxy solution.
H	Migration / IT Infrastructure shifting	• To develop a migration strategy for shifting the IT infrastructure of the OICL to the new co-hosted data centre. • Shift the specified IT infrastructure at the DC and DRC
I	Facility Management Services	• 24x7 Onsite Support • Advanced monitoring, resolution and reporting services.
J	Desktop	• 16 Desktops for FMS Resources at DC and DR Sites
K	Buyback	• The Bidder is required to buyback the specified existing hardware mentioned in the Inventory List in Annexure-7.

4. Scope of Work

OICL has outlined its vision for a Technology Refresh and other solutions implementation. This vision would involve a major transformation of the current information technologies ('IT'). With this objective, OICL is floating this Request for Proposal ('RFP') to address its requirements.

The Bidder should be a well-qualified total solution provider to implement the initiative successfully. The Bidder should be capable of providing a total integrated solution as part of this RFP. The Bidder should have executed similar implementations in the past and have adequate experience of the same.

The contract duration would be for 6 years from the date of signing the contract. OICL can further extend this at its discretion at the same or better mutually agreed terms and conditions. However for TCO purposes, the period for commercial evaluation is 6 years.

4.1 General

4.1.1. The Bidder shall be responsible for Supply, Installation, Implementation, Migration and Support of IT Infrastructure Solutions i.e. Servers, Storage, Tape Library, Disk based appliance, Network Switch, Firewall, Server Load Balancer, Application Delivery Controller, Racks, KVM Switch, Desktop mentioned in the Bill of Material at DC and DR sites with one year warranty and undertake AMC of these equipment for next five years after expiry of the one-year warranty period.

4.1.2. The Bidder shall be responsible for supply, installation, configuration, migration, testing and commissioning the Mail Messaging Solution for 18000 users and maintain the same during the tenure of the contract.

4.1.3. The Bidder shall implement the DR management tool with all the necessary processes, parameters and DR drills to ensure the proper functioning of the DR site with respect to various parameters like RPO, RTO etc.

4.1.4. Currently OICL has a DC Site at Bengaluru and DR Site at Vashi (Navi Mumbai). However, OICL has floated a separate RFP for DC and DR Co-Hosting Services. The Bidder shall be responsible for the seamless migration of the specified infrastructure from existing sites to the new sites which will be located in the same cities i.e. Bengaluru and Mumbai/Navi Mumbai respectively. The Bidder is also required to buyback the specified inventory as mentioned in Annexure-7. Buy back items are available at OLD DC and DR. However, buy back is subject to OICLs discretion. If any item is required for future use, OICL may remove it from buy-back offer. Bidder has to collect item in as-is-where-is condition. No additional expenses will be paid for removal of items. Destruction of hard disks and magnetic tapes should be done in the presence of OICL representative. The commercials quoted by the Bidder should include the buyback price assessed by the Bidder.

4.1.5. The Bidder shall refer to Annexure 1 – Minimum Technical Specifications, the Bidder should ensure that the proposed components are in compliance with the technical requirements stated in that Annexure and provide their compliance.

4.1.6. Bidder has to propose a detailed solution document in line with the scope of work asked in this tender bringing out the detailed DC and DR high level and low level architecture along with the DR Plan. This document should also clearly articulate various aspects involved in DC-DR operations like RPO, RTO, DC-DR replication, backup and restoration planning etc.

4.1.7. The Bidder should deliver all the equipment at new DC and DR Sites within 8 weeks from the issue of Purchase Order by OICL.

4.1.8. The Bidder shall be responsible for structured LAN and SAN cabling at DC and DR Sites. Entire cabling should be dressed and labelled as per industry standards. The cables shall be required to have different colour codes for better identification. The cabling shall include

the accessories required for structured LAN and SAN cabling. The same shall be maintained during the contract period.

4.1.9. Bidder must take the complete responsibility of supply and commissioning of the hardware, software and other equipment i.e. the entire scope of work of this tender.

4.1.10. An annual audit should be done by the OEM for the proposed security infrastructure at the DC and DR sites.

4.1.11. The Bill of Materials as estimated by OICL is not exhaustive. Any additional items/ components like Hardware, Software, any licenses, accessories, service etc. as required to make the project completely operational may be assessed by the Bidder and the same may be incorporated in the offer. Even at the time of execution, if any additional items/ components like Hardware, Software, any licenses, accessories, service etc. are required to complete the system integration, notwithstanding the BOM as identified by the Bidder as above, the same shall be provided at no additional cost to OICL.

4.1.12. The tentative DC and DR layout architecture is mentioned in Annexure-10, however the Bidder is expected to study and submit the detailed DC and DR Logical and Physical Layout along with Network design diagram.

4.1.13. The Bidder shall also deliver a presentation to the OICL IT team at New Delhi before and after Implementation of the setup at DC and DR Site which should cover the detailed architecture and deployment.

4.2 Storage

4.2.1. Existing Storage Details

OICL has a heterogeneous storage environment. OICL's existing storage details are mentioned in the table below:

4.2.1.1. Existing SAN Storage

S.N.	Location	Make & Model	RAW Capacity (in TBs)	Year of Purchase	Action
1	DC, Bangalore	ST9990V	33	2009	Buyback and Data Migration to New Storage
2	DC, Bangalore	EMC VMAX 20K	100	2013	Re-Use, Data Migration to New Storage & restoration of data from new storage.
3	DR, Vashi	EMC Clarrion AX4	20	2011	Re-Use and Shifting to OICL HO
4	DR, Vashi	EMC VMAX 20K	100	2013	Re-Use, Data Migration to New Storage & restoration of data from new storage.

4.2.1.2. Existing SAN Switches

S.N.	Location	Make & Model	Qty	Year of Purchase	Action
1	DC, Bangalore	Brocade DS 5300	2	2013	Re-Use
2	DC, Bangalore	Brocade5100	2	2009	Buyback
2	DR, Vashi	Brocade DS5300	2	2013	Re-Use
4	DR, Vashi	Silkworm 4100	2	2004	Buyback

4.2.1.3. Existing FCIP Routers

S.N.	Location	Make & Model	Qty	Year of Purchase	Action
1	DC, Bangalore	Brocade 7500	2	2009	Buyback
2	DR, Vashi	Brocade 7500	2	2007	Buyback

4.2.1.4. Application Mapping on EMC VMX Storage

S.N.	Application	Usable Capacity (Bengaluru)	Usable Capacity (Vashi)
1	INLIAS	12 TB (DC)	12 TB (DR)
2	INLIAS Reporting	NA	12 TB (DC)
3	HRMS	5 TB (DC)	NA
4	SAP	5 TB (DC)	5 TB (DR)
5	Web Portal	5 TB (DC)	5 TB (DR)

4.2.2. Scope of Work for Storage

4.2.2.1. The Bidder shall be responsible for the Supply and Installation of Enterprise Storage System, SAN Switches and FC-IP Routers at DC and DR Sites.

4.2.2.2. Physical shifting of EMC VMAX from old DC to New DC. Migration of data from existing EMC VMAX Storage to new Storage. Further, few applications might be reverted back to the existing EMC VMAX Storage from new storage. Responsibility of EMC VMAX space allocation etc. also rests with Bidder thereafter, for the contract period. Onsite FM will be with bidder. However, remote management will remain with OEM. AMC is already in place with M/s Sify.

4.2.2.3. Creation of LUN and mount points and allocation of resources based on the requirement.

4.2.2.4. Carry out changes in mount points, storage allocations, during installation and support periods to fulfill system requirements

4.2.2.5. Integration of existing and new SAN Switches with the existing as well new Servers, Storage, Tape Library and Disk based backup Solution. Further Bidder shall integrate all future infrastructure procured by OICL in coordination with the supplier.

4.2.2.6. Integration of FC-IP Routers with Storage Systems.

4.2.2.7. Patch update & version upgrade of software & firmware.

4.2.2.8. Provide 24x7 support service available from the concerned OEM.

4.2.2.9. The following table specifies the quantity of equipment required:

S.N.	Product	DC Site	DR Site
1	Enterprise Storage System	1	1
2	SAN Switch	2	2
3	FC-IP Routers	2	2

4.3 Servers

4.12.1 Bidder should Supply, Install, Implement, Maintain and Support Intel servers at DC and DRS along with Operating System and undertake AMC of these equipment for five years after expiry of the one-year warranty period.
4.12.2 Bidder should provide 24x7 support service available from the concerned OEM.
4.12.3 Bidder should apply all software updates / version upgrades released by the respective OEM.
4.12.4 Bidder should perform Change Management activities through onsite visit or remote access
4.12.5 Bidder should conduct quarterly review of performance of equipment under AMC.
4.12.6 The bidder shall be required to perform above tasks, render requisite services, make available resources, any additional hardware, software, licenses or cables as may be required for the successful implementation of the complete solution at no additional cost to OICL.

4.4 Network & Security

OICL wishes to procure network & security infrastructure. The selected Bidder would be taking over the existing equipment (buy-back) placed in the OICL's current DC & DR Sites and would be replacing them with new infrastructure. The Bidder shall ensure:

4.4.1. Supply and Installation of Networking and Security (Core Switch, DMZ Switch, Distribution Switch, Core Firewall, DMZ Firewall, SLB, ADC) Infrastructure at DC and DR Sites.

4.4.2. Seamless transition from the existing network & security infrastructure to the proposed network & security infrastructure with minimal service disruption.

4.4.3. Installation of Network and Security components in high availability with necessary configuration.

4.4.4. Implementing redundant networking including VLANs as per requirement.

4.4.5. Set up of DMZ Zone(s) and internal zone (s).

4.4.6. Set up of Management system and Reporting services.

4.4.7. Patch update and version upgrade of the software as and when released by the OEM.

4.4.8. Provide 24x7 support service available from the concerned OEM.

4.4.9. Following table specifies the quantity of equipment required:

S.N.	Product	DC Site	DR Site
1	Core Switch	2	2
2	DMZ Switch	2	2
3	Distribution Switch	4	4
4	Core Firewall with integrated IPS	2	2
5	DMZ Firewall with integrated IPS	2	2
6	Server Load Balancer	2	2
7	Application Delivery Controller	2	2

4.5 Backup Solution

The Bidder shall be responsible for Supply, Installation, Integration, Rollout, Operational configuration, failover testing and Maintenance of total solution for implementation of Backup solution at DC and DR. The Bill of Material (BOM) has already been provided in the document. Scope for the Bidder shall be the following but not limited to:

a) A Complete end to end implementation of the solution including hardware and software of in-scope items.
b) The Bidder shall be responsible for setting up backup infrastructure for enabling online backup for ready restores and a vaulting option for data continuity. OICL shall assist the Bidder by providing feasible setup needs.
c) The Bidder will configure the backup server and software to enable automated backup of all applications as per OICL's requirement based on parameters finalized by OICL. The Backup Server, Tape Library & Disk Based Backup Solution is required to be configured to existing SAN box as well as new Enterprise Storage System at both DC & DR sites.
d) The Bidder shall provide the architecture of the proposed backup and recovery solution include features and functionality designed to minimize the impact on production servers, applications, and network bandwidth and ultimately the end user of the production environment.
e) The Bidder should be responsible for resolving any compatibility issues with the existing hardware and software infrastructure during deployment of the backup solution.
f) The Bidder shall be responsible for ensuring that the backup and restoration process is executed in the prescribed timeframe and is encrypted before being backed up on to the tapes. The backup must be done using latest backup technologies having features such as encryption etc. to enable a secure, efficient and reliable backup and restoration process.
g) The Bidder shall be responsible for upgradation of backup software at OICL at no extra cost during the contract period. The Bidder shall manage the complete backup infrastructure & solution including hardware, software etc. for a period of 6 years.
h) The Bidder shall review the current backup policy of OICL and should recommend and implement the best practices as per current industry standards. OICL shall provide the details of the existing backup policy to the successful Bidder.
i) The Bidder shall be responsible for all patches/updates required in the offered solution for smooth installation of the backup solution without any extra cost to OICL.
j) The backup solution should be scalable and free from any restriction of including the number of applications and data size in the backup thus catering to such future needs of the OICL.
k) The proposed backup solution should have an integrated monitoring tool/portal to make an assessment of the uptime of the solution proposed. The integrated portal/tool facility of the proposed solution should be able to generate & send reports to assigned email-ids to proactively monitor the overall health of the solution. The Bidder shall be responsible for its installation and configuration, as per OICL's requirement, during AMC/Warranty period of the project, as applicable.
l) Though the sizing and architecture has been finalized by OICL, The Bidder must own the same and should get it vetted from the OEM for the specific Sizing Parameters and Architecture given above and suggest changes as required, if any, to meet the objective outlined in this document.
m) The hardware supplied by the Bidder should be robust and reliable, as per technical specifications. The Bidder must guarantee that all equipment delivered is brand new. Further all hardware and software to be supplied/delivered and installed must be of the latest version & IPv6 ready.

4.5.1 Tape Library

4.5.1.1. Following table specifies the current tape library details deployed at DC and DR sites:

S.N.	Location	Make & Model	Year of Purchase	Action
1	DC, Bangalore	SUN SL500 (LTO 4)	2009	Buyback, Data Migration to new Tape Library
2	DR, Vashi	SUN SL500 (LTO 3)	2007	Buyback, Data Migration to new Tape Library

4.5.1.2. The Bidder is required to supply, implement and maintain the tape library at the DC and DRC over the tenure of the contract.

4.5.1.3. The tape library offered shall be robotically controlled to identify media, load tape media into drives and put them back into corresponding shelves automatically.

4.5.1.4. It shall be supplied with encryption capable Linear Tape Open (LTO) Gen6 Tape Drives with 2500GB native and 6250 GB compressed capacity (when 2.5:1 compression is used).

4.5.1.5. The Offered Tape Library shall provide 8Gbps native FC connectivity to SAN switches.

4.5.1.6. Tape Library shall provide remote monitoring capability, redundant hot swap power supplies.

4.5.2 Disk Based Backup Solution

4.5.2.1. OICL expects the Bidder to position a disk based appliance. The Bidder also has to provision a solution for periodic backup on tapes and offsite the same as per the policy of the OICL. The backup on the tape should support encryption so that in case of physical loss of the tape the data cannot be read.

4.5.2.2. The appliance should use a de-duplication technology.

4.5.2.3. The appliance should be sized to provide a fast recoverability of data.

4.5.2.4. OICL is considering speeding up its backup operation, therefore the Bidder needs an appliance at DC and identical appliance at DR with replication enabled. The Bidder has to recommend appropriate bandwidth for the same.

4.5.2.5. The Bidder is required to design and size the Disk Based Backup Solution at the DC and DRC. Bidder is also required to supply, install, configure and provide onsite comprehensive warranty and AMC/ATS services for the same over the tenure of the contract.

4.5.3 Backup Software

4.5.3.1. Currently OICL is using the Symantec NetBackup Solution. OICL expects the Bidder to implement and support new backup software application which will meet the technical specifications mentioned in RFP.

4.5.3.2. The backup software should be able to take backups of Solaris, Windows, RHEL and OEL servers.

4.5.3.3. All backup/restore administration must be controlled by a centralized master system.

4.5.3.4. The software must be based on a Graphical User Interface (GUI) so that all backup servers can be managed centrally, regardless of location.

4.5.3.5. The Bidder has to implement and maintain the backup policy.

4.6 DR Management Solution

OICL envisages implementing a DR Management Tool. The Bidder is required to design, supply, Install, configure, test, implement, monitor, maintain and provide Facilities Management for the DR Management tool.

4.6.1. Deployment of a fully functional DR Solution.
4.6.2. Proposed DR solution architecture including details of solution component.
4.6.3. Solution design and demonstrate compliance to RTO (2 Hour) / RPO (1 Hour) for OICL's IT Systems and other Functional and Technical requirements mentioned in this document.
4.6.4. The tool should be capable to provide Day-to-day Verification and Analysis of IT Changes
4.6.5. The tool should provide facility for Data center Change Management & Auditing.
4.6.6. The tool should provide a wide array of DR compliance reports that can be generated on demand to help assess and analyze current ability to maintain business continuity.

4.7 Mail Messaging Solution

Bidder shall design, supply, install, configure, migrate, test and commission the Mail Messaging Solution and maintain the same during the tenure of the contract. Bidder has to ensure that the mail messaging system is integrated with Core Insurance & other required applications. The number of email user is 18,000. The email solution proposed by the Bidder should comply with all the requirements mentioned in this RFP.

4.7.1. Currently OICL is using Sun Communication Express for the mail messaging solution. For E-mail Client, OICL is using Microsoft Outlook 2007/2010/2013, Windows Live-Mail. The proposed solution support and compatible to all these clients.
4.7.2. User Categorization for proposed solution shall be as per following table:

	Tier-1	Tier-2	Tier-3	Tier-4	Tier-5
No. of Users	8000	5000	2000	2000	1000
Average No. of Mails/ User/ Day (incoming and outgoing)	50	100	150	200	200
Avg. Size of mail (kb)	50	50	100	100	150
Allocated Space	200 MB	500 MB	1 GB	1.5 GB	2 GB
Attachment Size	10 MB	10MB	10MB	10MB	10MB

4.7.3. The Bidder shall be responsible for implementation of the Centralized Mail Messaging Solution with High Availability for 18000 users. Number of Front-end Client Licenses required is 11000. The Bidder shall be responsible for Supply, Installation, Migration, Integration, Rollout, Operationalization, Failover Testing and Maintenance of total solution comprising Hardware, Storage and Software. Currently count of desktops is approximately 13000 across all OICL offices in India.
4.7.4. Installing and configuring the Mail Messaging solution at Data Centre (DC) and Disaster Recovery site (DRS) will be part of the Bidder's scope. Mail is required with HA at DC and without HA at DR site.
4.7.5. The Bidder shall be responsible for setting up infrastructure for publishing OICL Email services to Internet and securing the same w.r.t messaging services. OICL shall assist the Bidder by providing IP link, networking equipment and interfacing with ISP provider for DNS record publishing and other setup needs.

4.7.6. The Bidder shall be responsible for setup/configuration of existing Email/SMTP Gateway Appliance i.e. TrendMicro IMSVA (with Anti-Virus & Anti-Spam capabilities). The Bidder would need to integrate the same with the proposed Mail/Messaging Solution.

4.7.7. The Bidder shall be responsible for setup/configuration of Email Access using Client (over Internet), Browser & Mobile Devices.

4.7.8. The Bidder shall be responsible for installation of Mail/Messaging Client at User Desktop/Laptop so that they are able to use all the features of the proposed Mail/Messaging Solution.

4.7.9. The Bidder shall be responsible for migration of user mailboxes from the existing Mail/Messaging Platforms to the proposed Mail/Messaging System. During the migration of the user mailboxes the Bidder shall ensure to minimize the end user impact as much as possible. If there is any issue involved in migration Bidder shall discuss the same with OICL and will plan accordingly. There should not be any data loss during migration.

4.7.10. As email would be a business critical application, OICL desires to implement the Email solution so as to optimally utilize the bandwidth by providing high availability and redundancy for the critical mailboxes. OICL wishes to implement an integrated and highly robust email anti-spam and anti-virus solution for all the email communication.

4.7.11. E-mails for 30 Days should be available online. Older emails should be moved to an online archive for 6 years.

4.7.12. The Bidder is required to quote for client server licenses for the mail messaging solution along with web based solution.

4.7.13. OICL has already factored the storage capacity in the required storage as part of this RFP, however the Bidder shall provide sizing for servers and storage required at DC and DR site as per Annexure-8.

4.8 Bulk (Volume) Mail

4.8.1. Bidder shall provide Bulk (Volume) Mail service at hosted model.

4.8.2. The approximate count of bulk mail per day is twenty thousand; accordingly the Bidder shall design and propose the solution.

4.8.3. Each Bulk Mail may contain a PDF attachment.

4.9 Proxy Server/ Appliance

4.9.1. The solution should run on physical server/appliance.

4.9.2. The proposed solution should support a minimum of 4000 concurrent users from day one.

4.9.3. The solution should be deployed in High Availability (HA) Mode at DC and Non-HA Mode at DR Site.

4.9.4. The Bidder has to provide required hardware with adequate hardware sizing for smooth operation of the offered solution as the part of technical bid.

4.9.5. Bidder shall integrate proxy solution with existing Anti-Virus and URL filtering gateway (TrendMicro IWSVA)

4.10 Support during Warranty & AMC Period

The Bidder shall undertake to provide an onsite comprehensive 1 Year Warranty and AMC for next 5 years for all supplied Hardware and Software. The Bidder has to do on-site comprehensive maintenance of all in-scope components at Bengaluru and Vashi Data Centers.

4.10.1 The solution shall be under a comprehensive on-site warranty covering all parts / components, for a minimum period of one year from the date of acceptance of solution at DC and DR, whichever is later. The warranty will be expiring on the last day of that month and AMC will commence from the 1st of the month immediately following the month in which the warranty

period expires. The Warranty (ATS/AMC) should be back to back from OEM and comprehensive in nature.

4.10.2 Spares and support for the hardware/software should be available for a minimum of six years (one year warranty, five years AMC) from the date of acceptance of Solution at DC and DR, whichever is later.

4.10.3 During the period of warranty and AMC, it will be mandatory on the part of the Bidder to attend and resolve breakdown calls (if any) as per the parameters/ time-frame defined in the SLA Section 7 of this document. Breakdown penalty (if any) will be charged as per the terms defined in SLA section. The Bidder shall provide the support services like repair, replacement to resolve the problem as per the service levels.

4.10.4 In the event maintenance/ repair of any unit is to be carried out at any location outside OICL premises, the Bidder shall make all arrangements for removal and transportation of equipment to such location and back to OICL location at their risk and cost and will hand over the systems in 100% working condition after repair/maintenance. A standby of the same Make/ Model/ configuration or of higher configuration should be provided whenever such removal of installed equipment is taken away by Bidder for repair/maintenance, failing which, penalty as per provisions of SLA will be applicable. If the supplied equipment is to be replaced permanently due to the Bidder's inability to provide spares or maintain the equipment, the Bidder shall replace it with equipment of the same Make/ Model/configuration or of higher configuration. However, OICL may accept different make/model/ configuration at its discretion if the original make/model/ configurations are not available in the market due to obsolescence or technological up gradation.

4.10.5 The Bidder shall provide post implementation support, management and administration of software by applying software patches/ service packs and keep the solution updated or upgraded with the functionalities; compression-protocol updates etc. to latest version without any additional cost to OICL.

4.10.6 OICL will not be liable to pay any additional amounts in respect of any sort of maintenance covered under the scope of this tender during the tenure of the contract. Free on-site maintenance services shall be provided by the Bidder during the period of warranty.

4.10.7 During the Warranty & AMC period, the Bidder will have to undertake system maintenance and replacement or repair of defective server equipment.

4.10.8 Upon receipt of such notice the Bidder shall, as mentioned below, repair or replace the defective goods or parts thereof, without any cost to OICL.

4.10.9 If during operation, the downtime of any piece of equipment or component thereof does not prove to be within reasonable period (as per the SLA), the Supplier shall replace the unit of component with another of the same performance and quality or higher, at no cost to OICL

4.10.10 Further provided that OICL may, during the currency of the warranty, shift the goods wholly or in part to other location(s) within the Country and in such case the Supplier undertakes to continue to warrant or maintain the goods at the new location without any other additional cost to OICL.

4.10.11 Exclusions: In case of partial/ full damage or loss of equipment due to reasons beyond the control of OICL like (a) accident or negligence by OICL, (b) causes external to the equipment such as electrical power fluctuations and failures etc. (c) Theft, fires, riots, strikes or acts of enemy etc., the Bidder would not be penalized. However, the onus of such proof will be on the Bidder. In such circumstances also, the Bidder should be in a position to supply a functional standby equipment with same configuration or higher and restore all the services. Monthly rental of 5% of the equipment cost for that particular equipment / component will be payable by OICL to the Bidder for the equipment supplied as standby in lieu of the lost/ damaged equipment. No AMC will be paid by the standby equipment. Also AMC (if any) for the Lost/ Damaged equipment shall cease immediately. Fresh Order will be placed by OICL with the Bidder for the supply of the lost / damaged equipment as per the approved rates.

4.11 AMC of Existing Oracle T4 Servers

4.11.1. Bidder shall undertake AMC for existing Oracle T4-2 Servers for next 6 Years.
4.11.2. AMC should be back to back from each OEM and comprehensive in nature.
4.11.3. During the period of AMC, it will be mandatory on the part of the Bidder to attend and resolve breakdown calls (if any) as per the parameters/ time-frame defined in the SLA Section 7 of this document. Breakdown penalty (if any) will be charged as per the terms defined in SLA section. The Bidder shall provide the support services like repair, replacement to resolve the problem as per the service levels.
4.11.4. Bill of Material:

S.N.	Product Description	Unit Qty	Total Qty
	SPARC T4-2 server: family (1239BDY1FD, 1239BDY1FE, 1239BDY1FF, 1239BDY200)		
1	SPARC T4-2 server: base with 2 SPARC T4 8-core 2.85 GHz processors for non-EU countries	1	4
2	One 300 GB 10000 rpm 2.5-inch SAS-2 HDD	4	16
3	Two 8 GB DDR3-1066 registered DIMMs	16	64
4	Power cord: India, 2.5 meters, IS1293 plug, C13 connector, 10 A	2	8
5	StorageTek 8 Gb Fibre Channel PCIe HBA dual port QLogic	2	8
6	Sun Quad-port Gigabit Ethernet Adapter UTP	1	4

4.12 Migration

The Bidder shall be responsible for migrating the specified equipment at OICL's primary data center (Bengaluru) and disaster recovery site (Navi Mumbai) from their existing location to new locations within the same cities. The Bidder shall be responsible for documenting a plan for migration of required equipment and data from existing systems to new systems at DC and DR sites and submit the same to OICL with the technical bid.

4.12.1 Details of various applications, application vendor, current and to-be landscape is provided in Annexure-9 of this RFP. Successful Bidder shall co-ordinate with all the existing vendors of OICL during migration.
4.12.2 The Bidder shall be required to migrate the data from different systems which are currently installed at existing DC and DR sites to the new sites.
4.12.3 The Bidder shall ensure the data on the existing systems at DC and DR sites is not tampered with, deleted or altered under any circumstances.
4.12.4 The Bidder shall ensure full backup of all the data before commencing the transfer of data to new systems at DC and DR sites with the co-ordination of existing application vendors.
4.12.5 The Bidder shall solely be responsible for recovery of any missing / corrupt data on the new system at DC and DR Sites.
4.12.6 The Bidder is responsible for copying all the existing data from the existing systems to the new systems at DC and DR sites, based on the approved data migration plan.
4.12.7 The Bidder shall maintain records confirming successful data migration to new systems at DC and DR Sites; and submit the same to OICL.

4.12.8 The Bidder shall confirm and demonstrate that the migrated data is accessible to the respective users and data security is not compromised with the co-ordination of existing application vendors.

4.12.9 Downtime allowed for each application is not more than 12 hours and OICL shall prefer this switch over down time on weekends only.

4.12.10 Bidder has to factor the required additional infrastructure on rental basis for seamless migration. As per OICL's observation, total 12 core Routers (6 at DC & 6 at DR) shall be required which should be of similar capability and configuration. However, any other equipment required also to make the project completely operational may be assessed by the Bidder and the same may be incorporated in the offer.

4.13 Facility Management Services

This section describes, but does not limit itself to, the services required by OICL for the solution proposed as part of this RFP at the Data Centre, Disaster Recovery Site and OICL Offices. OICL intends that the contract which is contemplated herein with the Bidder shall be for a period of six years (6 years) from the date of signing the contract, and shall cover all Deliverables and Services required to be procured or provided by the Bidder during such period of contract. The Bidder needs to consider and envisage all services that would be required in the maintenance of the facilities. FM for all purposes means all Annual Maintenance Contract (AMC), warranties, ATS (Annual Technical Support) for all solutions, software's and interfaces provided, quoted and developed by the Bidder and all other costs necessary and incidental for the maintenance and support of the infrastructure and equipment.

The Bidder is expected to develop a methodology for executing FM services for OICL based on the requirements. The personnel being deployed by the Bidder for FM at the OICL should be employees of the Bidder's firm.

This section is broadly divided into following three sub-sections:

1. Services to be Implemented by Bidder at DC and DR Site
2. 24 x 7 Onsite Support
3. Advanced Monitoring, Reporting & Resolution Services

4.13.1. Services to be Implemented by Bidder at DC and DR Site

In line with the scope of work mentioned in sections above, the Bidder has to carry out the following work on all the supplied items:

4.13.1.1. Servers

i. Installation of servers with necessary configuration.
ii. Changes in configuration of physical / virtual instances during the installation and support period to fulfill the requirements of the system.
iii. Patch updates of software & firmware.

4.13.1.2. Storage, SAN Switch & FC-IP Routers

i. Installation of storage systems with necessary configuration based on the finalized design.
ii. Connectivity of storage with all the servers of OICL.

iii. Creation of LUN and mount points and allocation of resources based on the requirement.
iv. Carry out changes in mount point, storage allocations during installation and support period to fulfill system requirement
v. Patch updates & version upgrades of software & firmware.

4.13.1.3. Backup System

i. Finalize backup plan and configure systems based on the backup plan.
ii. Installation of tape library, disk based appliance and backup software.
iii. Monitoring of the backup, in case there is any failure to take corrective action.
iv. Periodic mock restoration activity to ensure that backup is effective.

4.13.1.4. DR Management Tool

i. Installation of DR Management Tool
ii. Setting up of RPO & RTO monitoring
iii. Carry out regular mock drills
iv. Carry out periodic Switching from DC to DR
v. Preparation of Standard Operating Procedure for Business continuity in case of disaster

4.13.1.5. Network Switch (Core Switch, Distribution Switch and DMZ Switch)

i. Installation of Network Switches with the necessary configuration.
ii. Implementation of redundant networking including VLANs as per requirement.
iii. Set up of management system and reporting services.
iv. Integration with the Firewall, SLB and ADC as applicable and configuration of relevant parameters for monitoring.
v. Patch update and version upgrade as and when released by the Network Switch OEM.
vi. Configuration of Routes, ACL and other policies viz. QOS etc. based on the requirement and its fine tuning
vii. Throughput testing of the Network switches if required.

4.13.1.6. Core and DMZ Firewall

i. Installation of Network firewalls in High availability with necessary configuration.
ii. Set up of DMZ Zone(s) and internal zone (s).
iii. Deployment of configuration based on agreed security policy.
iv. Setting up Log configuration.
v. Setup of Firewall Management System and Reporting services.
vi. Patch update and version upgrade of the firewall software as and when released by the Firewall OEM.
vii. Throughput testing of the Firewall if required.

4.13.1.7. Intrusion Prevention System

i. Installation of IPS with necessary configuration.
ii. Implementing redundant networking.
iii. Deployment of configuration based on agreed security policy Implementing automatic updation of the Signatures.

iv. Custom signature deployment as and when required by OICL.
v. Setting up Log configuration.
vi. Setup of IPS Management System and Reporting Services.
vii. Patch update and Version upgrade of the software as and when released by the OEM.
viii. Throughput testing of the IPS if required.

4.13.1.8. Server Load Balancer & Application Delivery Controller

i. Installation of SLB & ADC with necessary configuration.
ii. Configuration based on agreed deployment plan.

4.13.2. 24 x 7 Onsite Support

The Bidder shall deploy 24 x 7 dedicated certified onsite resources at DC and DR Site for regular maintenance support of the systems for complete duration of contract from the date of installation.

Location	Support Level	No. of Shifts on All Days	Minimum Resources in each Shift
DC	L1	3	3
DR	L1	3	3

The numbers provided above are only a minimum and the bidder may deploy more manpower to meet all Service Level requirements specified in the RFP. These resources should be field engineers of L1 level with the ability to resolve any severity issues that may arise during the period. The engineers deployed for the job at DC and DR Site must have suitable qualifications, experience and certification for the assigned job. The minimum required qualification of FMS engineers is BE/B.Tech/MCA with minimum three years of relevant experience in a FMS in a similar setup. The engineers shall be required to undertake the responsibilities of System Administrator and Trouble shooting of multi-brand Hardware (Server, Storage, Backup, Network, Security, and Mail Messaging etc.) Proposed Resources should have following skill sets:

i. RHEL Operating System (x86 Servers)
ii. Windows Operating System (x86 Servers)
iii. Proposed & Existing Storage Systems
iv. Proposed Backup Solution
v. Proposed Network Infrastructure
vi. Proposed Security Infrastructure
vii. Proposed Mail Messaging Solution
viii. Proposed DR Management Solution

4.13.2.1. Server Management and Administration

i. Monitoring of proposed systems and solutions as well as existing Cisco & HP Intel blade servers for key events, health and performance.
ii. Port monitoring: HTTP/HTTPS, DNS, SMTP, POP3, FTP, TCP ports, etc. are to be monitored continuously to ensure network and applications are up and running.
iii. Manage Operating System: This shall include support of Operating System, format and reinstallation of OS as requested by OICL, creation and maintenance of User Accounts,

Start / Stop service, OS debugging and recovery, maintenance of server logs, management of server disk space, addition or removal of Hardware or Software.

iv. The Bidder shall be responsible for a periodic health check of the systems, troubleshooting problems, analyzing and implementing rectification measures.

v. Implement and maintain standard operating procedures for maintenance of the infrastructure based on the policies provided by the purchaser and based on the industry best practices. Create and maintain documentation / checklists for the same.

vi. The Bidder shall be responsible for managing the user names, roles and passwords of all the relevant subsystems, including, but not limited to servers, devices, etc. The Bidder shall be responsible for management of passwords for all relevant components and devices under his purview and implement a password change mechanism in accordance with the security policy of the purchaser.

vii. The server administrators should regularly monitor and maintain a log of the performance monitoring of servers including but not limited to monitoring CPU, disk space, memory utilization, I/O utilization, etc. The Bidder should also ensure that the bottlenecks in the infrastructure are identified and fine tuning is done for optimal performance.

viii. The administrators should adopt a defined process for change and configuration management in the areas including, but not limited to, changes in parameter settings for servers, operating system, devices, etc., applying patches, etc.

4.13.2.2. Storage and Backup Management

i. Monitoring proposed and Existing EMC SAN Storage for key events, health and performance

ii. Managing space allocation related issues.

iii. Periodic reporting of storage.

iv. Fabric Switch Administration

v. BCV & Clone Administration Performance Management

vi. The Bidder shall perform Tape and Disk backup as per the requirement of the OICL. This will include managing the disk based appliance, tape library, regular backup and restore operations and assuring security of the media through appropriate access control.

vii. Monitor and enhance the performance of scheduled backups, schedule regular testing of backups and ensure adherence to related retention policies.

viii. Ensure prompt execution of on-demand backups of volumes, files and database applications whenever required by the OICL or in case of upgrades and configuration changes to the system.

ix. Real-time monitoring, log maintenance and reporting of backup status on a regular basis. The administrators should ensure prompt problem resolution in case of failures in the backup processes.

4.13.2.3. Network Administration

i. The Bidder is responsible for monitoring and administering the network.

ii. The Bidder is responsible for creating and modifying VLAN, assignment of ports to appropriate applications and segmentation of traffic.

iii. Port monitoring: Monitor HTTP/HTTPS, DNS, SMTP, POP3, FTP, TCP ports, etc. are continuously to ensure network and applications are up and running.

iv. The Bidder shall be responsible for periodic health check of the systems, troubleshooting problems, analyzing and implementing rectification measures.

v. On an ongoing basis, the Bidder is responsible for troubleshooting issues in the infrastructure, network of OICL to determine the areas where fixes are required and ensuring resolution of the same.

vi. The network administrators should regularly monitor and maintain a log of the performance monitoring of the network.

vii. The network administrators should undertake a regular analysis of events and logs generated in all the sub systems. The administrators should undertake actions in accordance with the results of the log analysis.

viii. The network administrators should adopt a defined process for change and configuration management in the areas including, but not limited to, changes in parameter settings for devices, applying patches, etc.

ix. The network administrators are responsible for managing the trouble tickets, diagnosis of the problems, reporting, managing escalation, and ensuring rectification of problems as prescribed in the SLA.

x. Implement and maintain standard operating procedures for maintenance of the infrastructure based on the policies provided by the purchaser and based on the industry best practices. Create and maintain documentation / checklists for the same.

xi. The Bidder shall be responsible for managing the user names, roles and passwords of all the relevant subsystems, including, but not limited to appliances, servers, applications etc.

xii. The Bidder shall be responsible for management of passwords for all relevant components and devices under his purview and implement a password change mechanism in accordance with the security policy of the purchaser.

xiii. Regular updates, releases, patches, version upgrades, subscription, etc. for supplied software packages including Networking equipment,

xiv. Fault reporting facility with the OEM.

xv. Performance tuning, checking of system usage load and parameters for performance tuning of the offered Networking equipment.

4.13.2.4. Security Administration

i. The Bidder is expected to provide Security management services to maintain stipulated SLA.

ii. The Bidder should address ongoing needs of security management including, but not limited to, monitoring of various devices / tools such as firewall, intrusion detection, application delivery controller etc. through implementation of proper patches and rules.

iii. Maintain an updated knowledge base of all the published security vulnerabilities and virus threats.

iv. Ensure that patches / workarounds for identified vulnerabilities should be patched / blocked immediately.

v. Responding to security breaches or other security incidents and coordinate with respective OEMs in case a new threat is observed to ensure that a workaround / patch is made available for the same.

vi. Undertake maintenance and management of security devices, including, but not limited to maintaining firewall services to restrict network protocols and traffic, detecting intrusions or unauthorized access to networks.

vii. The Bidder should ensure that the security policy is maintained on an ongoing maintenance and updates to the same are made regularly.

viii. Firewall management: Initial setup of the firewall, implementation of rule base on the firewall to enable customer specific applications and ports, implementation of security policies based on services (HTTP, FTP, Telnet), source address / name, destination address/ name, online monitoring of firewall through a central console , system administration for firewall, including updates & hot fixes that affect its performance, changes in firewall rule base with proper change management and backup of firewall configuration each time there is a configuration change.

ix. Intrusion detection and prevention: Initial installation and setup; applying appropriate levels of risk assessment for specific needs which allow security policies to be an integral part of the scanning process; tracking of resource usage for anomalies and logging any suspicious packets from the outside; log maintenance and management; automated network based security assessment and policy compliance evaluation.
x. The Bidder shall also manage and monitor proposed Server Load Balancer and Advance Delivery Controller at both the sites.
xi. Regular updates, releases, patches, version upgrades, subscription, etc. for supplied software packages including Operating system of Security Devices.
xii. Performance tuning, checking of system usage load and parameters for performance tuning.

4.13.2.5. Messaging Administration

i. Administration of mail servers
ii. Monitoring performance and management of user account, mail boxes, post office and address book.
iii. Backup and archival management.
iv. Transaction log management.
v. Implementation of mail policies as defined by the OICL, including, but not limited to, user security, access control, encryption, mail box sizes, mail sizes, spam, content filtering, etc.
vi. Management and monitoring mail queues, mail routing of incoming and outgoing mail.

4.13.3. Advanced Monitoring and Reporting Services

Bidder shall provide 24X7 proactive monitoring services for following equipment available at OICL DC and DR Sites:

1. All Systems and Solution Proposed in this RFP.
2. Existing Cisco & HP Blade Servers as mentioned in the Inventory List available at DC and DR Sites.
3. Existing EMC VMAX 20K SAN Storage and Brocade SAN Switches available at DC and DR Sites.

This needs to be delivered via a network of remote engineers and worldwide remote monitoring centres that are designed for full disaster recovery. The services to be delivered to OICL via a remote gateway device. A single knowledge base, online portal and tool set needs to ensure that OICL business reaps the maximum benefit from the Bidder's global expertise. The Privacy and security needs to be designed into the architecture by making only information about the status of systems, not business data, available to Bidder.

This service needs to provide continuous monitoring of events, and will filter and qualify them, identifying events that need customer attention. The service needs to provide a secure, interactive web-based portal which serves as a critical link between Bidder and the OICL. All elements regarding life state, including performance reporting, incident tracking and remediation, change management, inventory management, configuration details, and account information, can be viewed through this single source. It needs to act as a repository for both Bidder and the OICL for contact information and escalation processes.

The service needs to address incident, change, and problem management, availability and performance reporting, and configuration management. Bidder shall provide the Services for each system listed in the "Scope of Work" (each such system, component, or application shall be referred to as a "Configuration Item," and, collectively, all Configuration Items shall be referred to as the "Environment") along with existing Intel blade servers and EMC SAN Storage. Bidder shall provide the Services using tools and systems (collectively, the "Mission Critical Support Platform"), including tools for collecting, storing, managing, updating, and presenting data about all Configuration Items and their relationships.

The Bidder shall be responsible to arrange any IT Infrastructure required delivering this service to OICL.

This service needs to **provide 99.5% uptime.**. This service from the Bidder should provide:

- Proactive Monitoring & management (24x7x365) as subscribed
- 15 min notification SLA
- Portal Dashboard for the service
- Continual optimization of environment
- Quarterly review of performance
- Prompt issue identification and resolution
- Helps in change management, incident management and process management

The service should provide following benefits to OICL:

Service	OICL Expectation
24 x 365 Monitoring of telemetry	Identification of life state events
Event filtering	Focus on critical events
Alerts when specific metrics exceeds predefined thresholds	Proactive notification of potential issues
Reporting on event management, performance and availability	Identification of patterns that may predict improperly tuned configuration items
Response Time SLAs	Reliable service delivery

4.14 Project Management

Bidder will deploy a project manager based at Delhi who will manage the project as a whole and act as an interface between OICL and the Bidder during the contract period. He will be single point of contact on behalf of Bidder. Project manager shall also be responsible for co-ordinating with OICL's existing hardware and application vendors. The project manager should have a minimum of 10 years' experience in executing and managing similar projects.

The Bidder should provide the detailed description for project management activities as part of the proposal in response and compliant to this RFP.

The Project Manager's responsibilities would primarily cover the following:

a) To ensure services delivery and resource management.

b) To prepare project plan, managing the contingencies & resource management while maintaining service delivery.

c) Risk identification and mitigation strategy.

d) To create a resource redundancy plan for better continuity and reliability of services.

e) Sharing knowledge and value addition with OICL IT team on a continuous basis.

f) Innovative and effective use of monitoring tools in delivering services

g) Overall responsibility for delivery of services as per Scope/ Statement of Work/s (SOW) and Service Level Agreement (SLA).

h) Maintain project communications with stakeholders of OICL

i) Provide strategic and tactical recommendations in relation to technology related issues and technology improvement.

j) Resolve deviations from the phased project plan.

k) Conduct regularly scheduled project status/ review meetings involving officials of the Bidder and OICL

l) Submission of all periodic reports

4.15 Documentation

4.15.1. Documentation along with Technical Bid

4.15.1.1. The Bidder shall submit a detailed plan for the implementation of this project at the submission of RFP, including but not limited to:

a. Individual tasks per stage
b. Timelines
c. Dependencies
d. Test scenarios

4.15.1.2. The Bidder shall ensure the technical documentation includes, but not limited to the following:

a. LAN Design Document
b. Overall DC and DR Architecture Diagram
c. Rack Layout
d. Detailed Description of Proposed Solution
e. Detailed step-by-step Migration Strategy

4.15.2. Documentation & Reports Post Award of PO

4.15.2.1. The selected Bidder shall perform an in-depth analysis of the existing system and shall submit a detailed plan for the implementation of this project, including but not limited to the following:

a. Project Plan detailing each task with target date and assigned resource persons including the plan for migration of existing infrastructure from Old DC to New DC and installation of all supplied items and integration with existing infrastructure at DC and DR Sites.
b. Final DC and DR Architecture Diagram
c. Detailed LAN Design Document
d. Physical layout plan of the racks at DC and DRS

Selected Bidder shall submit this document to OICL for review and any suggestions by OICL will be incorporated therein. Design document should be vetted by OEM's of respective components.

4.15.2.2. Post successful implementation, the Bidder shall prepare a **System Design Document** including but not limited to following:

a. Final DC and DR Architecture Diagram
b. Detailed LAN Design Document
c. Cabling and labeling details
d. Procedure for raising support tickets with OEM along with escalation matrix
e. Physical layout plan of the racks at DC and DRS
f. Device wise configuration details of active components deployed in the network
g. Installation and administration guide with a work instruction document, to build the System from scratch in the event of a major failure.
h. System data, configuration backup and restore procedure with a schedule based on OICL's business continuity requirements and industry best practices.
i. Design document should be vetted by OEM's of respective components.

Bidder shall periodically update System Design Document and maintain the version control throughout the contract period.

4.15.2.3. The selected Bidder shall also submit the disaster recovery documentation which shall include, but is not limited to the following:

a. Data Centre Failover and Failback Design and Implementation Details.
b. Disaster Recovery, failback and failover plans for all IT Systems at OICL
c. List of parameters to check if the failover / failback was successful such as detailed DR checklist
d. Detailed procedures to switch an IT system or the entire IT services from DC to DR Site and Procedure to failback to DC from DRC after the DC services are restored.
e. Issues and risks pertaining to the DR drill conduction.

4.15.2.4. Bidder shall submit the reports on a regular basis in a mutually decided format. Softcopy of these reports shall be delivered automatically via email at specific frequency and to the pre-decided list of recipients. Bidder shall submit certain information as part of periodic review as and when required by the OICL. Following is the indicative list of reports:

a. Daily reports (to be submitted on next working day)

- Log of backup and restoration undertaken.
- Summary of resolved, unresolved and escalated issues/complaints to OEMs
- Mail traffic report

b. Weekly Reports (to be submitted on the first working day of the following week)

- Summary of systems rebooted.
- Summary of issues /complaints logged with the OEMs.
- Summary of changes undertaken in the Data Centre including major changes like configuration changes, patch upgrades, database reorganization, storage reorganization, etc. and minor changes like log truncation, volume expansion, user creation, user password reset etc.

c. Monthly Reports (to be submitted by 10th of the following month)

- Component wise IT infrastructure availability and resource utilization.
- Summary of component wise Data Centre uptime.
- Log of preventive / scheduled maintenance undertaken.
- Configuration Management summary report.
- Change Management summary report.

- Service Level Management – priority/severity wise response and resolution.
- Service Failure Analysis, listing out escalations and downtime/outages, if any.

d. Account Dash Board, listing out:

- Planned activities carried out during the month.
- Unplanned activities carried out during the month.
- Activities planned but missed specifying the reasons.
- Challenges faced during the month.

4.16 Shifting of Hardware from one location to another

4.16.1 The Bidder will also be responsible for contracting with and providing a qualified company that is experienced and specializes in the relocation of data centers and handling of high-end computing equipment. bidder will be responsible for providing trained, knowledgeable, and experienced staff to effectively de-install, package, oversee the transport, then re-install all specified equipment included in all phases of the move. Bidder must use the OICL's existing maintenance providers for equipment that is maintained under support contract to ensure that those contracts are not compromised or invalidated.

4.16.2 Prior to the start of relocation activities, the Bidder is to provide a team to prepare the pathways for both the "origin" and "destination" locations to avoid any possible damage in the process of moving equipment, to include (but not limited to) floors, walls, elevators, etc.). This preparation shall be done to the satisfaction of OICL.

4.16.3 The Bidder shall ensure that appropriate equipment and moving materials are provided and used to move the applicable computing equipment from their existing location, to the transport vehicle, and ultimately to the new installation location.

4.16.4 Bidder shall also be responsible to take insurance on the moving equipment in the name of OICL. Insurance amount shall be paid by OICL on actuals.

5. Terms & Conditions

5.1 General

5.1.1 Definitions

OICL/ PURCHASER: Shall mean The Oriental Insurance Company Limited

5.1.2 Amendment to Bid Document

At any time prior to the deadline for submission of Bids, OICL may for any reason either on its own initiative or in response to a clarification requested by a prospective Bidder, modify the Bid Document, by amendment.

All prospective Bidders that have received the Bid Document will be notified of the amendment. The same will be binding on them. In order to allow prospective Bidders reasonable time in which to take the amendment into account in preparing their Bids, OICL may, at its discretion, extend the deadline for a reasonable period to be decided by OICL for the submission of Bids. Details will be communicated and published on our portal www.orientalinsurance.org.in.

5.1.2.1 OICL also reserves the right to change any terms and conditions of the RFP and its subsequent addendums as it deems necessary at its sole discretion. OICL will inform the Bidder about changes, if any before the deadline of bids submission.

5.1.2.2 OICL may revise any part of the RFP, by providing an addendum to the Bidder at stage till commercial bids are opened. OICL reserves the right to issue revisions to this RFP at any time before the deadline for bid submissions.

5.1.2.3 OICL reserves the right to extend the dates for submission of responses to this document.

5.1.2.4 **Preliminary Scrutiny –** OICL will scrutinize the offer to determine whether it is complete, whether any errors have been made in the offer, whether required technical documentation has been furnished, whether the documents have been properly signed, and whether items are quoted as per the schedule. OICL may, at its discretion, waive any minor non-conformity or any minor deficiency in an offer. This shall be binding on the Bidder and OICL reserves the right for such waivers and OICLs decision in the matter will be final.

5.1.2.5 **Clarification of Offer –** To assist in the scrutiny, evaluation and comparison of offer, OICL may, at its discretion, ask the Bidder for clarification of their offer. OICL has the right to disqualify the Bidder whose clarification is found not suitable to the proposed project.

5.1.2.6 OICL reserves the right to make any changes in the terms and conditions of purchase. OICL will not be obliged to meet and have discussions with any Bidder, and / or to listen to any representations.

5.1.2.7 **Erasures or Alterations –** The offer containing erasures or alterations will not be considered. There should be no hand-written material, corrections or alterations in the offer. Technical details must be completely filled up. Correct technical information of the product being offered must be filled in. Filling up of the information using terms such as “OK”, “accepted”, “noted”, “as given in brochure / manual” is not acceptable. OICL may treat the offers not adhering to these guidelines as unacceptable.

5.1.2.8 **Right to Alter Quantities –** OICL reserves the right to alter the requirements specified in the tender. OICL also reserves the right to delete or increase one or more items from the list

of items specified in the tender. OICL will inform the Bidder about changes, if any. In the event of any alteration in the quantities the price quoted by the Bidder against the item would be considered for such alteration. The Bidder agrees that the prices quoted for each line item & component is valid for period of contract and can be used by OICL for alteration in quantities. Bidder agrees that there is no limit on the quantities that can be altered under this contract. During the contract period the Bidder agrees to pass on the benefit of reduction in pricing for any additional items to be procured by OICL in the event the market prices / rate offered by the Bidder are lower than what has been quoted by the Bidder as the part of commercial offer. Any price benefit in the products, licenses, software, services & equipment should be passed on to OICL within the contract period.

5.1.3 Acceptance of the Solution

5.1.3.1. The solution will not be treated as complete if any part of hardware / software etc. is not delivered as per the timelines specified in RFP. In such an event, the supply will be termed incomplete and will not be accepted and warranty period will not commence besides OICL's right to invoke the penalties which will be prescribed in the contract.

5.1.3.2. There will be an acceptance test conducted by OICL or its nominated consultants after implementation of solution at DC and DR. In case of discrepancy in hardware & related software supplied & not matching the Bill of Materials or technical proposal submitted by the Bidder in their technical bid, the Bidder shall be given 6 weeks' time to correct the discrepancy post which OICL reserves the right to cancel the entire purchase contract and the Bidder should take back their equipment at their costs and risks. The test will be arranged by the Bidder at the sites in the presence of the officials of OICL and / or its consultants. The warranty for the equipment (including OS and hardware provided by the Bidder pursuant to this Agreement) will commence after acceptance testing. The tests will involve trouble-free operation of the complete system during UAT apart from physical verification and testing. There shall not be any additional charges for carrying out this acceptance test. OICL will take over the system on successful completion of the above acceptance test. The Installation cum Acceptance Test & Check certificates jointly signed by Bidder's representative and OICL's official or its authorized representative should be received at Head Office along with invoice etc. for scrutiny before taking up the request for consideration of payment.

5.1.4 Sub-contracts

In case sub-contracting any of the activities under the scope of this RFP is required, the Bidder needs to notify and take prior permission in writing from OICL. It is clarified that notwithstanding the use of sub-contractors by the Bidder, the Bidder shall be solely responsible for performance of all obligations under the RFP irrespective of the failure or inability of the subcontractor chosen by the Bidder to perform its obligations. The Bidder shall also have the responsibility for payment of all dues and contributions, as applicable including any statutory requirement and compliance. No additional cost will be incurred by OICL on account of sub-contract, if any.

5.1.5 Conditional bids

Conditional bids shall not be accepted on any ground and shall be rejected straightway. If any clarification is required, the same should be obtained before submission of bids.

5.1.6 Submission of Bids

The Bidders shall seal the envelopes containing Eligibility Bid / Technical Bid / Commercial bid. Envelopes shall be addressed to OICL at the address given; and bear the Project Name "RFP for Technology Refresh for DC and DR Infrastructure" - Eligibility Bid/ Technical Bid / Commercial Bid Tender No. OICL/HO/ITD/TECH-REFRESH/2015/01 Dated 28th August 2015. Envelopes should indicate on the cover the name and address of the Bidder. A Bidder shall submit only one proposal.

5.1.7 Performance Security

Within 15 days after the receipt of Notification of Award from OICL, the Bidder shall furnish performance security to OICL as per Appendix - 6, which shall be equal to 10 percent of the value of the contract - valid till date of expiry of six year Contract period in the form of a bank guarantee from a nationalized/ scheduled bank as per the norms laid by the RBI.

Failure by Bidder to submit the Performance security will result in invocation of Bid security held by the Company (OICL).

5.1.8 Pre-Bid Meeting

All queries/ requests for clarification from Bidders must reach us by e-mail (**tender@orientalinsurance.co.in)** or in person before 17:00 hours on 4th September 2015. Format for the queries / clarification is provided in "Appendix 3 - Query Format". No clarification or queries will be responded in any other format. OICL will respond to any request for clarification of the tender document in the pre-bid meeting to be held on 11th September 2015.

The Representatives of Bidders attending the pre-bid meeting must have proper authority letter to attend the same and must have purchased the Tender document.

Any modification to the Bidding Documents, which may become necessary as a result of the pre-bid meeting, shall be made by the Company exclusively through the issuance of an Addendum and not through the minutes of the pre-bid meeting.

5.1.9 Installation and Implementation

The Bidder shall be responsible for supply, installation and commissioning of the proposed solution with technical specification as mentioned in Annexure-1; and to undertake AMC of the same.

At the direction of OICL, the acceptance test of the solution shall be conducted by the successful Bidder in the presence of OICL's authorized representative(s) and/or any other team or agency nominated by OICL. All expenses for acceptance test shall be borne by the Bidder. The acceptance tests should include verification of documentation for equipment start-up procedures; shutdown procedures; configuration; failover testing and testing of all redundancies – verification of documented fail-over and restoration procedures. Draft Acceptance test procedure should be submitted by Bidder. The final acceptance test procedures will be discussed and mutually agreed after the implementation.

5.1.10 Delay in Bidder's performance

Implementation of the Solution and performance of service shall be made by the Bidder in accordance with the time schedule specified by OICL in the contract.

Any unexcused delay by the Bidder in the performance of his implementation/service/other obligations shall render the Bidder liable to any or all of the following sanctions: forfeiture of his performance security, imposition of liquidated damages, and/ or termination of the contract for default.

If at any time during performance of the contract, the Bidder should encounter conditions impeding timely implementation of the Solution and/or performance of services, the Bidder shall promptly notify OICL in writing of the fact of delay, its likely duration and cause(s), before the scheduled delivery / installation / implementation date. OICL shall evaluate the situation after receipt of the Bidder's notice and may at their discretion extend the Bidder's time for delivery / installation / implementation, in which case the extension shall be ratified by the parties by amendment of the contract. If the Bidder's request to delay the implementation of the Solution and performance of services is not found acceptable to OICL, the above mentioned clause would be invoked.

5.1.11 Payment terms

The Bidder must accept the payment terms proposed by OICL. The commercial bid submitted by the Bidder must be in conformity with the payment terms proposed by OICL. Any deviation from the proposed payment terms would not be accepted. OICL shall have the right to withhold any payment due to the Bidder, in case of delays or defaults on the part of the Bidder. Such withholding of payment shall not amount to a default on the part of OICL.

Item	Payment	Documents to be Submitted
Hardware	70% against Milestone-4 as mentioned in Section 1.7 (Delivery of Hardware at New DC and DR Site)	Confirmation letter/mail from OEM, Delivery Certificate, Performance Bank Guarantee, Agreement.
	15% against Milestone-6 as mentioned in Section 1.7 (Completion of all work at the DC and DR Sites)	Documentation, Installation report and ATR
	15% against Milestone-7 as mentioned in Section 1.7 (Successful DR drill and documentation)	Sign-off Letter
Software/ Licenses	100% against Milestone-4 (Software/Licenses delivery)	Confirmation letter/mail from OEM, Delivery Certificate, Performance Bank Guarantee, Agreement.
Implementation, Installation, Migration & Commissioning	100% Post Sign off.	Certificate from authorized OICL Official.
FMS	25% of the Annual Charges at the end of each quarter	Quarterly call reports, MIS Reports
AMC	25% of the Annual Charges at the end of each quarter	

5.1.12 Mode of Payment

OICL shall make all payments only through Electronic Payment mechanism (viz. ECS). Bidders should invariably provide the following particulars along with their offers:

a) Account Number and Type of Bank account (Current / Savings/Cash Credit).
b) IFSC / NEFT Code (11 digit code) / MICR code, as applicable, along with a cancelled cheque leaf.
c) Permanent Account Number (PAN) under Income Tax Act;
d) TIN/Sales Tax Registration Number (for supply of Goods) and Service Tax, Registration Number (for supply of Services), as applicable.
e) E-mail address of the Bidder / authorized official (for receiving the updates on status of payments).

5.1.13 Currency of Payments

Payment shall be made in Indian Rupees (INR) only.

5.2 Other RFP Requirements

a. The Head Office of OICL is floating this RFP. However, the Bidder(s) getting the contracts shall install and commission the solution, procured through this RFP, at OICL's DC and DR or at such centers as OICL may deem fit and the changes, if any, in the locations will be intimated to the Bidder.

b. The Bidder's representative and local office at New Delhi will be the contact point for OICL. The delivery status of equipment should be reported on a weekly basis.

c. Bidder should ensure that the hardware delivered to OICL including all components and attachments are brand new. In case of Software Licenses, the Bidder should ensure that the same is licensed and legally obtained with valid documentation made available to OICL.

d. OEM's Authorization Form – The Bidder should furnish separate letter from original equipment manufacturer in the format provided in Appendix 7 – OEM's Authorization provided along with this RFP for quoted item.

e. Quoting multiple options for any of the line item mentioned in the Bill of Material is not allowed.

f. Bidder may consider Open Source Software (OSS) along with Closed Source Software (CSS) while responding the RFP. Bidder shall provide justification for exclusion of OSS in their response in case they are providing CSS.

g. If an OEM is bidding directly then OEM cannot come through other bidders.

6. Terms of Reference ('ToR')

6.1 Contract Commitment

OICL intends that the contract, which is contemplated herein with the Bidder, shall be for a period of Six years. The contract period will start from the date of PO shared to Bidder by OICL.

6.2 Ownership, Grant and Delivery

The Bidder shall procure and provide a non-exclusive, non-transferable licenses to OICL for the Software to be provided as a part of this project. The Software should be assignable / transferable to any successor entity of OICL.

OICL reserves the right to use the excess capacity of the licenses supplied by the Bidder for any internal use of OICL or its affiliates, or subsidiaries at no additional cost other than the prices mentioned in the commercial bid. The Bidder agrees that they do not have any reservations on such use and will not have any claim whatsoever against such use of the hardware, licenses and infrastructure.

Further the Bidder also agrees that such use will not infringe or violate any license or other requirements

6.3 Completeness of Project

The project will be deemed as incomplete if the desired objectives of the project Section 4 – Scope of Work of this document are not achieved.

6.4 Assignment

OICL may assign the hardware and software provided therein by the Bidder in whole or as part of a corporate reorganization, consolidation, merger, or sale of substantially all of its assets. OICL shall have the right to assign such portion of the AMC services to any of the sub-contractors, at its sole option, upon the occurrence of the following: (i) Bidder refuses to perform; (ii) Bidder is unable to perform; (iii) termination of the contract with the Bidder for any reason whatsoever; (iv) Expiry of the contract. Such right shall be without prejudice to the rights and remedies, which OICL may have against the Bidder. The Bidder shall ensure that the said subcontractors shall agree to provide such services to OICL at no less favourable terms than that provided by the Bidder and shall include appropriate wordings to this effect in the agreement entered into by the Bidder with such sub-contractors. The assignment envisaged in this scenario is only in certain extreme events such as refusal or inability of the Bidder to perform or termination/expiry of the contract.

6.5 Canvassing/Contacting

Any effort by a Bidder to influence the Company in its decisions on Bid evaluation, Bid comparison or award of contract may result in the rejection of the Bidder's Bid. No Bidder shall contact the Company on any matter relating to its Bid, from the time of opening of Commercial Bid to the time the Contract is awarded.

6.6 Indemnity

The Bidder's should indemnify OICL (including its employees, directors or representatives) from and against claims, losses, and liabilities arising from:

a) Non-compliance of the Bidder with Laws / Governmental Requirements

b) IP infringement

c) Negligence and misconduct of the Bidder, its employees, and agents

Indemnity would be limited to court awarded damages and shall exclude indirect, consequential and incidental damages.

The Bidder shall not indemnify OICL for

(i) Any loss of profits, revenue, contracts, or anticipated savings or

(ii) Any consequential or indirect loss or damage however caused

6.7 Inspection of Records

All Bidder records with respect to any matters covered by this tender shall be made available to OICL or its designees at any time during normal business hours, as often as OICL deems necessary, to audit, examine, and make excerpts or transcripts of all relevant data. Said records are subject to examination. OICL's auditors would execute confidentiality agreement with the Bidder, provided that the auditors would be permitted to submit their findings to OICL, which would be used by OICL. The cost of the audit will be borne by OICL. The scope of such audit would be limited to Service Levels being covered under the contract, and financial information would be excluded from such inspection, which will be subject to the requirements of statutory and regulatory authorities.

6.8 Publicity

Any publicity by the Bidder in which the name of OICL is to be used should be done only with the explicit written permission of OICL.

6.9 Solicitation of Employees

Both the parties agree not to hire, solicit, or accept solicitation (either directly, indirectly, or through a third party) for their employees directly involved in this contract during the period of the contract and one year thereafter, except as the parties may agree on a case-by-case basis. The parties agree that for the period of the contract and one year thereafter, neither party will cause or permit any of its directors or employees who have knowledge of the agreement to directly or indirectly solicit for employment the key personnel working on the project contemplated in this proposal except with the written consent of the other party. The above restriction would not apply to either party for hiring such key personnel who (i) initiate discussions regarding such employment without any direct or indirect solicitation by the other party (ii) respond to any public advertisement placed by either party or its affiliates in a publication of general circulation or (iii) has been terminated by a party prior to the commencement of employment discussions with the other party.

6.10 Information Ownership

All information processed, stored, or transmitted by Bidder equipment belongs to OICL. By having the responsibility to maintain the equipment, the Bidder does not acquire implicit access rights to the information or rights to redistribute the information. The Bidder understands that civil, criminal, or administrative penalties may apply for failure to protect information appropriately.

6.11 Sensitive Information

Any information considered sensitive must be protected by the Bidder from unauthorized disclosure, modification or access.

Types of sensitive information that will be found on OICL systems the Bidder may support or have access to include, but are not limited to: Information subject to special statutory protection, legal actions, disciplinary actions, complaints, IT security, pending cases, civil and criminal investigations, etc.

6.12 Confidentiality

Bidder understands and agrees that all materials and information marked and identified by OICL as 'Confidential' are valuable assets of OICL and are to be considered OICL's proprietary information and property. Bidder will treat all confidential materials and information provided by OICL with the highest degree of care necessary to insure that unauthorized disclosure does not occur. Bidder will not use or disclose any materials or information provided by OICL without OICL's prior written approval.

Bidder shall not be liable for disclosure or use of any materials or information provided by OICL or developed by Bidder which is:

a. possessed by Bidder prior to receipt from OICL, other than through prior disclosure by OICL, as documented by Bidder's written records;

b. published or available to the general public otherwise than through a breach of Confidentiality; or

c. obtained by Bidder from a third party with a valid right to make such disclosure, provided that said third party is not under a confidentiality obligation to OICL; or

d. Developed independently by the Bidder.

In the event that Bidder is required by judicial or administrative process to disclose any information or materials required to be held confidential hereunder, Bidder shall promptly notify OICL and allow OICL a reasonable time to oppose such process before making disclosure.

Bidder understands and agrees that any use or dissemination of information in violation of this Confidentiality Clause will cause OICL irreparable harm, may leave OICL with no adequate remedy at law and OICL is entitled to seek to injunctive relief.

Nothing herein shall be construed as granting to either party any right or license under any copyrights, inventions, or patents now or hereafter owned or controlled by the other party.

The requirements of use and confidentiality set forth herein shall survive the expiration, termination or cancellation of this tender.

Nothing contained in this contract shall limit the Bidder from providing similar services to any third parties or reusing the skills, know-how, and experience gained by the employees in providing the services contemplated under this contract. The confidentiality obligations shall survive for a period of one year post the termination/expiration of the Agreement.

6.13 Technological Advancements

The hardware and software proposed as part of this contract

a. should not reach end of support during the period of contract

b. should not have been announced End of Life /Sales

In the event if the proposed hardware and software reached end of support during the period of contract, in such case the Bidder is required to replace the end of support hardware/ software at no cost to OICL

6.14 Liquidated Damages

If the Bidder fails to deliver and power on the equipment as per Milestone -5 as per Section 1.7, OICL shall without prejudice to its other remedies under the contract, deduct from the contract price, as

liquidated damages, a sum equivalent to 0.5% of the contract price for every week (seven days) or part thereof of delay, up to maximum deduction of 10% of the contract price. Once the maximum is reached, OICL may consider termination of the contract.

6.15 Guarantees

Bidder should guarantee that all the software's provided to OICL are licensed and legal. All hardware and related software must be supplied with their original and complete printed documentation.

6.16 Termination for Default

OICL may, without prejudice to any other remedy for breach of contract, by 30 calendar days written notice of default sent to the Bidder, terminate the contract in whole or in part:

a) If the Bidder fails to deliver any or all of the Solution and services within the time period(s) specified in the contract, or any extension thereof granted by OICL; or
b) If the Bidder fails to perform any other obligation(s) under the contract

In the event of OICL terminating the contract in whole or in part, pursuant to above mentioned clause, OICL may procure, upon such terms and in such manner, as it deems appropriate, goods and services similar to those undelivered and the Bidder shall be liable to OICL for any excess costs incurred for procurement of such similar goods or services (capped at 5% differential value). However, the Bidder shall continue performance of the contract to the extent not terminated.

6.17 Force Majeure

The Bidder shall not be liable for forfeiture of his performance security, liquidated damages or termination for default, if and to the extent that, his delay in performance or other failure to perform his obligations under the contract is the result of an event of Force Majeure.

For purposes of this clause, "Force Majeure" means an event beyond the control of the Bidder and not involving the Bidder and not involving the Bidder's fault or negligence and not foreseeable. Such events may include, but are not restricted to, acts of OICL either in its sovereign or contractual capacity, wars or revolutions, fires, floods, epidemics, quarantine restrictions and freight embargoes.

If a Force Majeure situation arises, the Bidder shall promptly notify OICL in writing of such conditions and the cause(s) thereof. Unless otherwise directed by OICL, the Bidder shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.

6.18 Termination for Insolvency

OICL may, at any time, terminate the contract by giving written notice to the Bidder, without any compensation to the Bidder, whatsoever if:

i. The Bidder becomes bankrupt or otherwise insolvent, provided that such termination will not prejudice or affect any right of action or remedy which has accrued or will accrue thereafter to OICL.

ii. the Supplier being a company is wound up voluntarily or by the order of a court or a receiver, or manager is appointed on behalf of the debenture/shareholders or circumstances occur entitling the court or debenture/shareholders to appoint a receiver or a manager, provided that such termination will not prejudice or affect any right of action or remedy accrued or that might accrue thereafter to the OICL.

6.19 Termination for Convenience

Either party may, by 30 calendar days written notice sent to the other party, terminate the contract, in whole or in part at any time of their convenience. The notice of termination shall specify the extent to which performance of work under the contract is terminated, and the date upon which such termination becomes effective.

The goods and services that are complete and ready for shipment within 30 calendar days after the receipt of notice of termination by the Bidder shall be purchased by OICL at the contracted terms and prices. For the remaining goods and services, OICL may elect:

i. To have any portion completed and delivered at the contracted terms and prices; and/ or
ii. To cancel the remainder and pay to the Bidder a mutually agreed amount for partially completed goods and services and for materials and parts previously procured by the Bidder.

6.20 Resolution of disputes

OICL and the Bidder shall make every effort to resolve amicably, by direct informal negotiation between the respective project managers of OICL and the Bidder, any disagreement or dispute arising between them under or in connection with the contract. If OICL project manager and the Bidder project manager are unable to resolve the dispute they shall immediately escalate the dispute to the senior authorized personnel designated by the Bidder and OICL respectively. If after thirty days from the commencement of such negotiations between the senior authorized personnel designated by the Bidder and OICL, OICL and the Bidder have been unable to resolve amicably a contract dispute; either party may require that the dispute be referred for resolution through formal arbitration. All questions, claims, disputes or differences arising under and out of, or in connection with the contract or carrying out of the work whether during the progress of the work or after the completion and whether before or after the determination, abandonment or breach of the contract shall be referred to arbitration by a sole Arbitrator acceptable to both parties failing which the number of arbitrators shall be three, with each side to the dispute being entitled to appoint one arbitrator. The two arbitrators appointed by the parties shall appoint a third arbitrator who shall act as the presiding arbitrator. The Arbitration and Reconciliation Act, 1996 or any statutory modification thereof shall apply to the arbitration proceedings and the venue of the arbitration shall be New Delhi .The arbitration proceedings shall be conducted in English language. Subject to the above, the courts of law at New Delhi alone shall have the jurisdiction in respect of all matters connected with the Contract. The arbitration award shall be final, conclusive and binding upon the Parties and judgment may be entered thereon, upon the application of either Party to a court of competent jurisdiction. Each Party shall bear the cost of preparing and presenting its case, and the cost of arbitration, including fees and expenses of the arbitrators, shall be shared equally by the Parties unless the award otherwise provides.

6.21 Governing Language

The contract shall be written in the language of the bid i.e. English. All correspondence and other documents pertaining to the contract, which are exchanged by the parties, shall be written in that same language. English Language version of the contract shall govern its implementation.

6.22 Applicable Law

The contract shall be interpreted in accordance with the Indian Laws for the time being in force and will be subject to the exclusive jurisdiction of Courts at Delhi (with the exclusion of all other Courts)

6.23 Prices

The prices quoted (as mentioned in Appendix 01- Bill of Materials submitted by the Bidder) for the solution and services shall be firm throughout the period of contract and shall not be subject to any escalation.

6.24 Taxes & Duties

The Bidder shall be entirely responsible for all taxes, duties, license fees, and demurrage charges etc., incurred until delivery of the contracted goods & services to OICL. However, Octroi / local levies (if any), in respect of transaction between OICL and Bidder, will be reimbursed by OICL, on submission of proof of actual transaction. If there is any increase/decrease in taxes/ duties due to any reason whatsoever, after Notification of Award, the same shall be passed on to OICL.

6.25 Deduction

Payments shall be subject to deductions (such as TDS) of any amount, for which the Bidder is liable under the agreement against this tender.

6.26 No Claim Certificate

The Bidder shall not be entitled to make any claim whatsoever against OICL under or by virtue of or arising out of this contract, nor shall OICL entertain or consider any such claim, if made by the Bidder after he shall have signed a "No Claim" certificate in favour of OICL in such forms as shall be required by OICL after all payments due to the Supplier are made in full.

6.27 Rights reserved by OICL

i. Company reserves the right to accept or reject any or all Bids without assigning any reasons.
ii. Company reserves the right to verify the validity of information given by the Bidders. If at any future point of time, it is found that the Bidder had made a statement, which is factually incorrect, OICL will reserve the right to debar the Bidder from bidding prospectively for a period to be decided by OICL and take any other action as maybe deemed necessary.
iii. OICL reserves the right to issue a fresh RFP for this project at any time during the validity of the contract period with the selected Bidder.

6.28 Limitation of Liability

Bidder's cumulative liability for its obligations under the contract shall not exceed the total contract value and the Bidder shall not be liable for incidental / consequential or indirect damages including loss of profit or saving.

6.29 Waiver

No failure or delay on the part of either party relating to the exercise of any right power privilege or remedy provided under this tender document or subsequent agreement with the other party shall operate as a waiver of such right power privilege or remedy or as a waiver of any preceding or succeeding breach by the other party nor shall any single or partial exercise of any right power privilege or remedy preclude any other or further exercise of such or any other right power privilege or remedy provided in this tender document all of which are several and cumulative and are not exclusive of each other or of any other rights or remedies otherwise available to either party at law or in equity.

6.30 Violation of terms

OICL clarifies that OICL shall be entitled to an injunction, restraining order, right for recovery, suit for specific performance or such other equitable relief as a court of competent jurisdiction may deem necessary or appropriate to restrain the Bidder from committing any violation or enforce the performance of the covenants, obligations and representations contained in this tender document. These injunctive remedies are cumulative and are in addition to any other rights and remedies OICL may have at law or in equity, including without limitation a right for recovery of any amounts and related costs and a right for damages.

Successful Bidder has to enter into service level agreement with OICL and SLA should cover the following:

6.31 Repeat Order

OICL may place Repeat Order against the original order for a quantity up to 50% of the original order quantity within six months of placing the original order.

7. Service Level Agreement

The purpose of this Service Level Agreement (hereinafter referred to as SLA) is to clearly define the levels of service which shall be provided by the Bidder to purchaser for the duration of this contract. The benefits of this SLA are to:

- Trigger a process that applies Bidder's and Purchaser's attention to an aspect of performance when that aspect drops below an agreed upon threshold, or target.
- Makes explicit the expectations that Purchaser has for performance from the Bidder. The Bidder and Purchaser shall review the performance of the services being provided by the Bidder and the effectiveness of this SLA.

Definition:

For purposes of this Service Level Agreement, the definitions and terms as specified in the contract along with the following terms shall have the meanings set forth below:

i. "**Availability**" shall mean the time for which the services and facilities are available for conducting operations from the equipment hosted in the Data Centre and Disaster Recovery Sites.

ii. **"Downtime"** is the time the services and facilities are not available and excludes the scheduled outages planned in advance for the Data Centre.

iii. **"Scheduled Downtime"** is planned downtime that is included in the design of the system. Usually, for an activity such as software upgrade, preventive maintenance or any other planned downtime mutually agreed upon by the Bidder along with Purchaser.

iv. "**Incident**" refers to any event / abnormalities in the functioning of the Data Centre Equipment / remote site equipment/Services that may lead to disruption in normal operations of the Data Centre services.

v. "**Service Window**" shall mean the duration for which the facilities and services shall be available at the Data Centers. Service window in this case shall be 24x7x365.

Category of SLAs:

This SLA document provides for minimum level of services required as per contractual obligations based on performance indicators and measurements thereof. The Bidder shall ensure provisioning of all required services while monitoring the performance of the same to effectively comply with the performance levels. The services provided by the Bidder shall be reviewed by purchaser that shall:

i. Regularly check performance of the Bidder against this SLA.
ii. Discuss escalated problems, new issues and matters still outstanding for resolution.
iii. Review of statistics related to rectification of outstanding faults and agreed changes.
iv. Obtain suggestions for changes to improve the service levels.

S.N.	Items	Measurement	Expected Minimum Availability (in %)	Actual Availability (in %)	Non Performance Deductions
1	All equipment supplied as part of the RFP at DC and DR Sites i.e. Servers, Storage, SAN Switch, FC-IP Routers, Tape Library, Disk Based Appliance, Core Switch, Distribution Switch, Core Firewall, DMZ Firewall, Server Load Balancer, ADC, Proxy, Messaging Solution & DR Management Solution etc.	Availability of equipment at DC and DR	99.50%	< 99.5	1% of the total cost of the equipment for 6 years
				< 99.0	2% of the total cost of the equipment for 6 years
				< 98.5	3% of the total cost of the equipment for 6 years
				< 98.0	4% of the total cost of the equipment for 6 years
				< 97.5	5% of the total cost of the equipment for 6 years
2	Resource Availability				If the resource availability is less than 99%, then payment shall be deducted based on the pro-rata basis. (Total FMS cost per day divided by nos. of persons deployed)

Definitions

Non-Availability: Is defined as, the service(s) is not-available.

Severity Level 1: Is defined as, the Service is available but the critical redundant components have failed and there is urgent need to fix the problem to restore the service to the high availability Status or more than 50% users are affected.

Severity Level 2: Is defined as, the service is available but there is compromise on the features available in the Equipment / system and are required to fix the problem to bring the service to Normal Level.

Severity Level 3: Is defined as, the moderate degradation in the application performance No implications on the data integrity. Has no impact on the normal operations/day-to-day working. It has affected or may affect, <10% of the user community.

Severity Level 4: Equipment/system/Applications are stable and have no impact on the day-to-day working. It has affected or may affect a single user. For example, Account lockouts, Unable to open files, related calls.

Resolution Time: Represents the period of time from the problem occurrence to the time in which the root cause of the problem is removed and a permanent fix has been applied to avoid problem reoccurrence.

Recovery Time: Represents the period of time from the problem occurrence to the time in which the service returns to operational status. This may include temporary problem circumvention / workaround and does not necessarily include root cause removal.

Response Time: Represents the period of time from the problem occurrence to the time when

the problem is first attended by the Bidder's engineer.

Service	Severity	Response Time (Max)	Recovery Time (Max)	Resolution Time (Max)
Mail Servers, Backup Server, any other Server supplied	Non Availability & Severity 1	15 minutes	2 hours	1 day
	Severity 2	1 hour	4 hours	2 day
	Severity 3	2 hour	6 hour	2 day
	Severity 4	4 hour	8 hour	2 day
Storage System (Storage, SAN Switch, FC-IP Routers etc.)	Non Availability & Severity 1	15 minutes	2 hours	1 day
	Severity 2	1 hour	4 hours	2 day
	Severity 3	4 hour	12 hour	2 day
	Severity 4	10 hour	1 day	3 day
Backup Solution Including Tape Library and Disk based Appliance	Non Availability & Severity 1	15 minutes	2 hours	1 day
	Severity 2	1 hour	4 hours	12 hour
	Severity 3	4 hour	12 hour	1 day
	Severity 4	10 hour	1 day	2 day
Network and Security System (Switches, Firewalls, SLB, ADC etc.)	Non Availability & Severity 1	15 minutes	2 hours	1 day
	Severity 2	1 hour	4 hours	1day
	Severity 3	2 hour	6 hour	2 day
	Severity 4	4 hour	8 hour	2 day

The violation of any of the above SLA's in a quarter will attract a penalty as set out in the table below:

No. of SLA Violation in First Year	% of Deduction (of Total 1st Year Revenue)
3-5	0.5
5-10	1.5
10-20	2.5
More than 20	5

No. of SLA Violation in a Quarter (From 2nd Year to End of 6th Year)	% of Deduction (Of Total Quarterly Revenue)
3-5	0.5
5-10	1.5
10-20	2.5
More than 20	5

Uptime Calculation for the quarter:

{[(Actual Uptime + Scheduled Downtime) / Total No. of Hours in a Quarter] x 100}

8. Instruction to Bidders

8.1 Procedure for submission of Bids

The Bidders will be required to submit following three documents in three separate envelopes.

1. Eligibility Bid
2. Technical Bid
3. Commercial Bid

Three sealed envelopes containing hard copies of pre-qualification bid, technical bid and commercial bid along with Soft copies should be submitted in the following manner:

Envelope I – Two hard copies (spirally bound) of pre-qualification bid in the format given in this tender, with information requested by OICL along with EMD in the form of Bank Guarantee and 1 compact disk (CD) containing the soft copy of pre-qualification bid.

a) Each of the two hard copies of pre-qualification bid should be a complete document, bound as a volume and placed in separate sealed envelopes super-scribed Pre-qualification Bid for Tender No. OICL/HO/ITD/ TECH-REFRESH /2015/01 Dated 28th August 2015
b) Each of the sealed envelopes should also be marked as “Original” and “First Copy” respectively.
c) The two envelopes of pre-qualification bid should be placed in a single sealed envelope and super-scribed as: Pre-qualification Bid for Tender No. OICL/HO/ITD/ TECH-REFRESH /2015/01 dated 28th August 2015

Envelope II - Technical bid comprising of two spirally bound hard copies of the technical bid in the format given in this tender, along with 1 compact disk (CD) containing the soft copy of technical bid.

a) Each of the two hard copies of technical bid should be a complete document, bound as a volume and placed in separate sealed envelopes super-scribed Technical Bid for Tender No: OICL/HO/ITD/ TECH-REFRESH /2015/01 dated 28th August 2015
b) Each of the sealed envelopes should also be marked as "Original" and "First Copy" respectively.
c) The two envelopes of technical bid should be placed in a single sealed envelope super-scribed: Technical Bid for Tender No: OICL/HO/ITD/ TECH-REFRESH /2015/01 dated 28th August 2015
d) Soft copy of the response to the technical bids should also be provided in MS excel/MS word. The soft copy is to be placed in Technical Bid. In case of any discrepancies between the hardcopy and softcopy OICL will use the hardcopy submitted by the Bidder for the evaluation. THE SOFT COPY SHOULD NOT CONTAIN COMMERCIALS AND COMMERCIALS ARE TO BE ENCLOSED ONLY IN COMMERCIAL BID COVER. A masked copy of Appendix 1- bill of material should be a part of technical bid.
e) The Bidders have to note that the technical proposal must contain Soft copy of the technical bid only. Soft copy of the commercial bid should not be enclosed with technical bid.

Envelope III - Two spirally bound hard copies of commercial bid in the format given in this tender, along with 1 compact disk (CD) containing the soft copy of the commercial bid.

a) Each of the two hard copies of the commercial bid should be a complete document, bound as a volume and placed in separate sealed envelopes super-scribed Commercial Bid for Tender No: OICL/HO/ITD/ TECH-REFRESH /2015/01 dated 28th August 2015
b) Each of the sealed envelopes should also be marked as "Original" and "First Copy" respectively.
c) The two envelopes of commercial bid should be placed in a single sealed envelope super-scribed: Commercial Bid for Tender No: OICL/HO/ITD/ TECH-REFRESH /2015/01 dated 28th August 2015
d) Soft copy of the commercial bid should also be provided in MS excel format. The soft copy is to be placed in commercial bid. In case of any discrepancies between the hardcopy and softcopy OICL will use the hardcopy submitted by the Bidder for the evaluation.

Note:

1. The Bid shall be typed in English and signed by the Bidder or a person duly authorized to bind the Bidder to the Contract. The person(s) signing the Bids shall initial all pages of the Bids.
2. All envelopes should be securely sealed and stamped.
3. It is mandatory for the Bidder to quote for all the items mentioned in the RFP.

8.2 Bid Security

EMD of ₹ 4,00,00,000/- (Rupees Four Crores Only) in the form of Bank Guarantee favoring 'The Oriental Insurance Company Ltd' valid for six months should be submitted as per format given in Appendix 5 - Pro forma for Bid Security.

a) BG should be drawn on Nationalized / Scheduled bank in favour of 'The Oriental Insurance Company Ltd'. Non-submission of BG along with Eligibility-Bid document will disqualify the Bidder.
b) BG will be returned to the qualified Bidder after acceptance of Purchase Order and/ or Signing of the Contract(s) by the Bidder and submission of required Performance Bank Guarantee (PBG) as per format given in Appendix 6 – Pro forma for Performance Security.
c) For the Bidders who do not qualify in this tender, BG will be returned after the selection of successful Bidder.
d) EMD submitted by Bidder may be forfeited if:
    i. Bidder backs out of bidding process after submitting the bids;
    ii. Bidder backs out after qualifying;
    iii. Bidder does not accept the Purchase Order / Sign the Contract within the time prescribed by OICL after qualifying.

9. Bid Documents

9.1 Eligibility Bid Documents

Eligibility document should contain following

1. Compliance to Eligibility Criteria along with Required Supporting Documents as per Section 1.6
2. The power of attorney or authorization, or any other document consisting of adequate proof of the ability of the signatory to bind the Bidder
3. EMD of ₹ 4,00,00,000/- (Rupees Four Crores Only) in the form of BG favoring 'The Oriental Insurance Company Limited' as per Appendix-5
4. Similar projects Undertaken in the previous five financial years.
5. Undertaking that the Bidder has quoted for all items and the bid validity will be for 180 days from the date of submission of commercial bid.
6. Manufacturer Authorization Form as per Appendix-7 for all supplied hardware and software.
7. Letter from OEM confirming availability of support from within India and various direct support options available with OEM.
8. Statement of No-Deviation as per Appendix-8
9. Eligibility bid compliance as per Appendix – 4.1
10. Application Form for Eligibility Bid

Note:

1. Participation in this tender will mean that the Bidder has accepted all terms and conditions and clauses of this tender and subsequent modifications to this tender, if any.
2. The documentary evidence asked in respect of the eligibility criteria would be essential. Bids not accompanied by documentary evidence may be subject to rejection. Clarification/ Additional documents, if any, sought by OICL from the Bidder has to be submitted within the stipulated time. Otherwise, bid will be rejected and no further correspondence in the matter will be entertained by OICL.
3. Any alterations, erasures or discrepancies in figures etc. may render the bid invalid. The bid may be rejected in case of non-adherence to any of the instructions given above.

9.2 Technical Bid Documents

Technical Bid should contain the following:

1. Executive Summary of Bidder's response: The Executive Summary should be limited to a maximum of five pages and should summarize the content of the response. IT should initially provide an overview of Bidder's organization and position with regards to proposed solution and professional services. A brief description of the unique qualifications of the Bidder should be included. Information provided in the Executive Summary is to be presented in a clear and concise manner.

2. Covering Technical Letter (Appendix 2) giving reference of this tender and consent for acceptance of all the Terms and Conditions of this tender.
3. Detailed Design Document:
    a. Understanding OICL's scope of work and requirements
    b. Detailed proposed solution with solution architecture.
    c. Key feature and functionalities of proposed products.
    d. Detailed Migration Methodology
    e. Proposed Facility Management Service
        - 24x7 onsite support experience
        - Advanced Monitoring and Reporting Service
4. Compliance to Minimum Technical Specifications as per Annexure-1 with cross reference to the data sheet / BoM for each point.
5. Part coded Technical Bill of Material of all the quoted components with unit and total quantity.
6. Datasheets of Proposed components.
7. Detailed Work Plan (Project Plan) for all the solution as mentioned in Section 4 "Scope of Work" and Section 1.7 "Project Timelines" of this document. A PERT chart or equivalent chart providing the delivery plan and scheduled date of commencement of delivery and completion of the delivery should also be provided.
8. CV's of Manpower proposed.
9. Masked Commercial Bid: The Bidder should also include a replica of the final commercial bid without prices in the technical bid. "The Bidder must note that the masked commercial bid should be actual copy of the commercial bid submitted with prices masked and not copy of the Pro-forma/format of the Appendix 1 – Bill of Materials in the RFP."
10. References to the previously executed projects as required in Annexure-4.
11. Technical bid compliance as per Appendix – 4.2

OICL reserves the right not to allow / permit changes in the technical specifications and not to evaluate the offer in case of non-submission or partial submission of technical details.

OICL may at its discretion waive any minor non-conformity in any offer and the same shall be binding on all Bidders and OICL reserves the right for such waivers.

If OICL is not satisfied with the technical specifications in any tender and observes major deviations, the technical bids of such Bidders will not be short-listed and the price bids of such Bidders will not be opened. No further discussions shall be entertained with such Bidders in respect of the subject technical bid.

9.3 Commercial Bid Documents

Commercial Bid should contain two hard copies and one soft copy of the Commercial-bid document as per Appendix 1 – Bill of Materials. The Commercial Bid should give all relevant price information and should not contradict the Technical Bid in any manner. There should be no hidden costs for items quoted.

The rates quoted should be in Indian rupees only and same should be rounded off to the nearest rupee and filled in both words and figures.

10. Evaluation Process

The competitive bids shall be submitted in three stages:

- Stage 1 – Eligibility Evaluation
- Stage 2 – Technical Evaluation
- Stage 3 – Commercial Evaluation

10.1 Eligibility Evaluation

Eligibility criterion for the Bidders to qualify this stage is clearly mentioned in Section 1.6 - Eligibility Criteria of this document. The Bidders who meet ALL these criteria would only qualify for the second stage of evaluation. The Bidder would also need to provide supporting documents for eligibility proof. All the credentials of the Bidder necessarily need to be relevant to the Indian market.

The decision of OICL shall be final and binding on all the Bidders to this document. OICL may accept or reject an offer without assigning any reason whatsoever.

10.2 Technical Evaluation

Total Marks 500. Minimum Overall Qualifying marks to become eligible for qualifying for Commercial Evaluation are 70% i.e. 350 out of 500.

Category	Criteria	Max Marks
A.	Bidders Project Experience	150
B.	Response to RFP & Design, Implementation & Project Management	200
C.	Bidders Technical Presentation	150
	Total	**500 Marks**

The break-up of the scoring is mentioned in the Bidder scoring chart - Annexure 2. It is mandatory for the Bidder to comply with all the line items given in the technical specifications (Annexure 1). In case if the Bidder does not comply with any of the line items given in technical specifications (Annexure 1), it will not qualify to Stage 3 of evaluation process even if they score the cut-off marks in Stage 2.

OICL at its discretion may reject the proposal of the Bidder, without giving any reason whatsoever, if in case the submission/responses received from the Bidder were found to be unsatisfactory.

10.3 Commercial Evaluation

The commercial bids for the technically qualified Bidders will be opened and reviewed to determine whether the commercial bids are substantially responsive. Bids that are not substantially responsive are liable to be disqualified at OICL'S discretion. The total cost of ownership for the purpose of evaluation shall be calculated over the contract period of 6 years.

OICL will award the contract to the successful Bidder whose bid has been determined to be substantially responsive and has been determined as the lowest commercial bid (L1), provided further that the Bidder is determined to be qualified to perform the contract satisfactorily.

11. Disclaimer

This RFP is being issued by OICL for inviting bids for Technology Refresh for DC & DR Infrastructure. The words 'Tender' and 'RFP' are used interchangeably to refer to this document. The purpose of this document is to provide the Bidder with information to assist in the formulation of their proposal. While the RFP has been prepared in good faith with due care and caution, OICL or any of its employees or consultants do not accept any liability or responsibility for the accuracy, reasonableness or completeness of the information contained in this document. The information is not intended to be exhaustive. Interested parties are required to make their own inquiries. OICL reserves the right not to proceed with the project, to alter the timetable reflected in this document or to change the process or procedure to be applied. It also reserves the right to decline to discuss the project further with any party submitting a bid. No reimbursement of any cost will be paid to persons, entities submitting a Bid.

12. Appendix

This Page is
Intentionally
Left blank

12.1 Appendix 1: Bill of Material

SUMMARY OF COSTS			
S.N.	**Table Reference**	**Items**	**Cost (INR)**
1.	**Table-A**	**DC Site Components**	
2.	**Table-B**	**DR Site Components**	
3.	**Table-C**	**Application Software**	
4.	**Table-D**	**Miscellaneous Items**	
5.	**Table-E**	**Facility Management Services**	
6.	**Table-F**	**Implementation and Migration Cost**	
7.	**Table-G**	**Optional Items**	
8.	**Table-H**	**Buy Back Cost**	
Grand Total - TCO for 6 Years (A+B+C+D+E+F+G-H)			

Grand Total in Words – (Rupees……)

Note:

1. All the prices of this document should flow correctly from the respective sheets.
2. The total cost should flow from the individual sheets within this Appendix.
3. Bidder should strictly follow the format given in Table.
4. OICL reserves the right to change the quantity of items quoted above at the time of placing order. In such case the value of the order will be the cost of items finally opted by OICL.
5. The warranty will start from the date of signing the ATR.
6. The Bidder is responsible for all the arithmetic computation and price flows. OICL is not responsible for any errors.
7. Optional Items (Table-G) shall be part of commercial evaluation; however OICL may or may not place the order for these components during the period of contract.

Table A – DC (Bengaluru) Site Components											
S.N.	Solutions	Make & Model	Unit Price	Qty	Amount with 1 year warranty (Including all taxes)	AMC (Excluding All Taxes)					Total Amount (6 years)
						2nd Year	3rd Year	4th Year	5th Year	6th Year	
1	Enterprise Storage System			1							
2	SAN Switch			2							
3	FC-IP Routers			2							
4	Tape Library			1							
5	Disk Based Backup Solution			1							
6	Backup Software			1							
7	Blade Chassis*										
8	Backup Server*										
9	Mail Servers*										
10	NOC & HRMS Reporting Servers			10							
11	Server - CTA			1							
12	Server - OEM			1							
13	Proxy Server / Appliance*										
14	Other Servers*										
15	Core Switch			2							
16	DMZ Switch			2							
17	Distribution Switch			4							
18	Core Firewall with IPS			2							
19	DMZ Firewall with IPS			2							
20	Server Load Balancer			2							
21	Application Delivery Controller			2							
22	42U Rack			6							
23	IP KVM Switch			2							
24	Desktop			8							
25	Any Other, (Please specify)*										
Table A - Total											

Table B – DR (Mumbai) Site Components											
S.N.	Solutions	Make & Model	Unit Price	Qty	Amount with 1 year warranty (Including all taxes)	AMC (Excluding All Taxes)					Total Amount (6 years)
						2nd Year	3rd Year	4th Year	5th Year	6th Year	
1	Enterprise Storage System			1							
2	SAN Switch			2							
3	FC-IP Routers			2							
4	Tape Library			1							
5	Disk Based Backup Solution			1							
6	Backup Software			1							
7	Blade Chassis*										
8	Backup Server*										
9	Mail Servers*										
10	NOC & HRMS Reporting Servers			4							
11	Server - CTA			1							
12	Server - OEM			1							
13	Proxy Server / Appliance*										
14	Other Servers*										
15	Core Switch			2							
16	DMZ Switch			2							
17	Distribution Switch			4							
18	Core Firewall with IPS			2							
19	DMZ Firewall with IPS			2							
20	Server Load Balancer			2							
21	Application Delivery Controller			2							
22	42U Rack			6							
23	IP KVM Switch			2							
24	Desktop			8							
25	Any Other, (Please specify)*										
Table B - Total											

Table C – Application Software											
S.N.	Solutions	Make & Model	Unit Price	Qty	Amount with 1 year warranty (Including all taxes)	AMC (Excluding All Taxes)					Total Amount
						2nd Year	3rd Year	4th Year	5th Year	6th Year	(6 years)
1	Mail Messaging Solution (For 18000 Users)										
2	Mail Client Access Licence			11000							
3	DR Management Solution*										
4	Any Other, (Please specify)*										
Table C - Total											

Table D – Miscellaneous Items (Excluding All Taxes)										
S.N.	Item	Unit Price	Qty	1st Year	2nd Year	3rd Year	4th Year	5th Year	6th Year	Total Amount (6 years)
1	Bulk (Volume) Mail Solution*									
2	AMC of Oracle T4 Servers		4							
3	Any Other, (Please specify)*									
Table D - Total										

Table E – Facility Management Services (Excluding All Taxes)										
S.N.	Item	Unit Price	Qty	1st Year	2nd Year	3rd Year	4th Year	5th Year	6th Year	Total Amount (6 years)
1	Onsite Support (Resources - DC)*									
2	Onsite Support (Resources - DR)*									
3	Project Manager		1							
4	Advanced Monitoring & Reporting Services		1							
5	Any Other, (Please specify)*									
Table E – Total										

Table F – Implementation and Migration Cost			
S.N.	**Components**	**Qty**	**Total Cost (Including all taxes)**
Implementation Cost for DC (Bengaluru) Components			
1	Enterprise Storage System	1	
2	SAN Switch	2	
3	FC-IP Routers	2	
4	Tape Library	1	
5	Disk Based Backup Solution	1	
6	Backup Software	1	
7	Blade Chassis*		
8	Backup Server*		
9	Mail Servers*		
10	NOC & HRMS Reporting Servers	10	
11	Server - CTA	1	
12	Server - OEM	1	
13	Proxy Server / Appliance*		
14	Other Servers*		
15	Core Switch	2	
16	DMZ Switch	2	
17	Distribution Switch	4	
18	Core Firewall with IPS	2	
19	DMZ Firewall with IPS	2	
20	Server Load Balancer	2	
21	Application Delivery Controller	2	
22	42U Rack	6	
23	IP KVM Switch	2	
24	Desktop	8	
25	Any Other, (Please specify)*		
Implementation Cost for DR (Mumbai) Components			
26	Enterprise Storage System	1	
27	SAN Switch	2	
28	FC-IP Routers	2	
29	Tape Library	1	
30	Disk Based Backup Solution	1	
31	Backup Software	1	
32	Blade Chassis		
33	Backup Server*		
34	Mail Servers*		
35	NOC & HRMS Reporting Servers	4	
36	Server - CTA	1	
37	Server - OEM	1	
38	Proxy Server / Appliance*		

39	Other Servers*		
40	DR Management Server*		
41	Core Switch	2	
42	DMZ Switch	2	
43	Distribution Switch	4	
44	Core Firewall with IPS	2	
45	DMZ Firewall with IPS	2	
46	Server Load Balancer	2	
47	Application Delivery Controller	2	
48	42U Rack	6	
49	IP KVM Switch	2	
50	Desktop	8	
51	Any Other, (Please specify)		
Implementation Cost for Application Software			
52	Mail Messaging Solution		
53	DR Management Solution		
54	Bulk (Volume) Mail Solution		
55	Any Other, (Please specify)		
Migration Cost			
56	Migration Activity at DC		
57	Migration Activity at DR		
58	Any Other, (Please specify)		
Table F – Total			

Table G – Optional Items (Excluding all taxes)			
S.N.	**Description**	**Qty**	**Total Cost**
1	**Enterprise Storage System**		
1a	Cost of 20 TB usable capacity with 900 GB or higher SAS Disks including necessary hardware & licenses	1	
1b	Cost of 20 TB usable capacity with 4 TB or higher NL-SAS Disks including necessary hardware & licenses	1	
1c	Cost of 5 TB usable capacity with 400 GB or higher SSD/ Enterprise Flash Disks including necessary hardware & licenses	1	
1d	Cost of additional 64 GB Cache for Enterprise Storage System	1	
1e	Cost of clone license in the increments of 20 TB	1	
1f	Cost of snapshot license in the increments of 20 TB	1	
1g	Cost of remote replication license in the increments of 20 TB	1	
2	**Backup**		
2a	Cost of 1 LTO-6 Drive	1	
2b	Cost of 20 LT0-6 Cartridges	1	
2c	Cost of 20 TB usable capacity using SATA/NL-SAS for Disk based backup	1	
2d	Cost of next 10TB backup software license	1	
3	**Mail Clients**		
3a	Front-end Mail Clients	2000	
4	**FMS**		
4a	Additional Onsite Support for one blade chassis with Intel Servers (Win/RHEL) – Per Site		
4b	Advanced Monitoring & Reporting Services for one blade chassis with Intel Servers (Win/RHEL)		
Table G - Total			

Table H – Buy Back Cost (Including all taxes)						
S.N.	**Model**	**Make**	**Qty**	**Purpose**	**Unit Price**	**Total Price**
Bengaluru Site						
Servers						
1	T5120	Sun	1	Mail MTA (DR)		
2	T5120	Sun	1	On-site T&D		
3	T2000	Sun	1	Not in Use		
4	T2000	Sun	1	Proxy BNG		
5	V480	Sun	1	Oracle Enterprise server		
6	M4000	Sun	1	Backup Server		
7	SB6000 Blade Chassis	Sun	1	Blade Chassis		
8	X6250 Blade	Sun	1	HRMS Reports		
9	X6250 Blade	Sun	1	HRMS T&D		
10	X6250 Blade	Sun	1	Antivirus Server		
11	X6250 Blade	Sun	1	SSP-DC-Mgmt		
12	X6250 Blade	Sun	5	SAP SERVER		
13	HCL Server	HCL	3	Not in Use		
14	SB6000 Blade Chassis	Sun	1	Blade Chassis		
15	SB X6270 M2 Blade	Sun	1	3i Infotech Web Services		
16	SB SPARC T3 Blade	Sun	1	HRMS Reporting Layer		
17	x4150	Sun	1	NET ADMIN		
Storage & Backup						
18	ST9990V	Sun	1	Sun-Storage		
19	SL500	Sun	1	Tape Library		
20	Brocade5100	Brocade	2	FC Switch		
21	Brocade 7500	Brocade	2	FCIP Router		
Desktops						
22	HP PC	PC	1	Solomon App Server		
23	PC-1	SUN PC	5	Onsite team		
24	Wipro Net	Wipro	1	HRMS Data Capturing		
Network & Security						
25	CISCO 6500-E	Cisco	2	Core Switch		
26	CISCO ASA 5580	Cisco	2	Firewall		
27	CISCO CATALYST 3750 G	Cisco	2	DMZ Switch		
28	Cisco IPS 4260	Cisco	2	IPS		
29	CISCO CATALYST 2950G	Cisco	1	L2 SWITCH		
30	CISCO ACE 4710	Cisco	2	SLB		
Mumbai Site						
Servers						
31	Sun-V490	Sun	1	Backup server		
32	SUN-V480-02	Sun	1	INLIAS Reporting		
33	SUN-E2900	Sun	2	INLIAS Reporting		
34	SE T5220	Sun	2	Mail server		
35	SUN-V480-03	Sun	1	Proxy server		

36	HCL 2700 CA	HCL	1	Trend Micro Control		
37	Sun Fire X4170 M2	Sun	1	CTA Server		
38	SUN-T5120	Sun	1	Web Portal server		
39	Sunblade6000 Chassis	Sun	1	Web Portal chassis		
40	SBT6320 Blade	Sun	7	Web Portal server Blade		
41	HCL 2700 BD-2	HCL	1	HCL helpdesk server		
42	Blade Chassis	HP	1	PC NOC		
43	Blade Server	HP	6	PC NOC		
44	HP DL580	HP	1	PC NOC		
45	Infiniti Global Line 2700ST	HCL	4	NOC server 1		
46	Infiniti Global Line 2700	HCL	1	SSP server		
47	HP ML 110	HP	1	FTP Server		
48	SUN-E2900	SUN	3	NOT IN USE		
Storage & Backup						
49	Silkworm 4100	Brocade	2	SAN switch A		
50	SUN-SL500	Sun	1	Tape Library		
51	Sun Tape Drive	Sun	2	DDS-4 tape drive		
52	SUN – L100	Sun	1	TAPE Library		
53	half height LTO-3	Quantum	1	External Tape Drive		
54	BrocadeSW7500	Brocade	2	FCIP Replication Router		
Network & Security						
55	CISCO-PIX 515 E	Cisco	2	DMZ Firewall		
56	Cisco 3750	Cisco	2	DMZ switch		
57	Cisco 6506	Cisco	2	Core switch		
58	Cisco 2950	Cisco	2	Management switch		
59	KVM switch		1	8 Ports KVM switch		
60	HCL-24TMS-2GCS	HCL	1	24 port switch		
61	CISCO ACE 4710	Cisco	2	SLB		
62	CISCO ASA 5585	Cisco	2	Core Firewall		
63	Cisco MCS 7800	Cisco	2	Call Manager		
Desktops						
64	Sun 150	SUN	1	Workstation		
65	HCL MONITOR	HCL	1	Console PC		
66	HP MONITOR-5500	HP	1	Monitor		
67	MONITOR	Compaq	1	Monitor		
Table H - Total						

(*Please mention the quantity as per proposed solution)

12.2 Appendix 2 : Covering Technical Offer

To

The Deputy General Manager
Information Technology Department,
The Oriental Insurance Company Limited,
2nd Floor, Head Office, “Oriental House”,
A-25/27, Asaf Ali Road,
New Delhi - 110 002

Dear Sir,

1. Having examined the Scope Documents including all Annexures and Appendices, the receipt of which is hereby duly acknowledged, we, the undersigned offer to supply and deliver all the items mentioned in the ‘Request for Proposal’ and the other schedules of requirements and services for your company in conformity with the said Scope Documents in accordance with the schedule of Prices indicated in the Price Bid and made part of this Scope.
2. If our Bid is accepted, we undertake to abide by all terms and conditions of this Scope and also to comply with the delivery schedule as mentioned in the Scope Document.
3. We agree to abide by this Scope Offer for 180 days after the last date of submission of commercial bid and our Offer shall remain binding on us and may be accepted by OICL any time before expiry of the offer.
4. This Bid, together with your written acceptance thereof and your notification of award, shall constitute a binding Contract between us.
5. We undertake that in competing for and if the award is made to us, in executing the subject Contract, we will strictly observe the laws against fraud and corruption in force in India namely “Prevention of Corruption Act 1988”.
6. We certify that we have provided all the information requested by OICL in the format requested for. We also understand that OICL has the exclusive right to reject this offer in case OICL is of the opinion that the required information is not provided or is provided in a different format.

Dated this……..by …….20

Authorised Signatory

(Name: Contact Person, Phone No., Fax, E-mail)
(This letter should be on the letterhead of the Bidder duly signed by an authorized signatory)
Signature and Seal of the Bidder

12.3 Appendix 3 : Query Format

S.N.	Page No.	Point / Section #	Existing Clause	Query Sought
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

12.4 Appendix 4 : Summary of Documents Submitted

4.1 – Eligibility Bid Compliance

S.N.	Documents	Compliance (Yes/No)
1	Compliance to Eligibility Criteria along with Required Supporting Documents as per Section 1.6	
2	The power of attorney or authorization, or any other document consisting of adequate proof of the ability of the signatory to bind the Bidder	
3	EMD of Rs. 4,00,00,000/- (Rupees Four Crores Only) in the form of BG favoring 'The Oriental Insurance Company Limited' as per Appendix-5	
4	Similar projects Undertaken in the previous five financial years.	
5	Undertaking that the Bidder has quoted for all items and the bid validity will be for 180 days from the date of submission of commercial bid.	
6	Manufacturer Authorization Form as per Appendix-7 for all supplied hardware and software.	
7	Letter from OEM confirming availability of support from within India and various direct support options available with OEM.	
8	Statement of No-Deviation as per Appendix-8	
9	Application Form for Eligibility Bid (Annexure-5)	

4.2 – Technical Bid Compliance

S.N.	Documents	Compliance (Yes/No)
1	Executive Summary of Bidder's response	
2	Covering Technical Letter (Appendix 2)	
3	Detailed Solution Architecture with Design Document	
4	Detailed Migration Strategy	
5	Compliance to Minimum Technical Specifications as per Annexure-1	
6	Part coded Technical Bill of Material	
7	Datasheets of Proposed components.	
8	Detailed Work Plan (Project Plan)	
9	CV's of Manpower proposed.	
10	Masked Commercial Bid (Appendix 1)	
11	References to the previously executed projects as required in Annexure-4.	

12.5 Appendix 5 : Pro forma for Bid Security

To: (Name of Purchaser)

Whereas _____ (hereinafter called 'the Bidder') has submitted its bid dated _____ for the _____. (hereinafter called "the Bid").

KNOW ALL MEN by these presents that WE _____ having our registered office at _____ (hereinafter called "the Bank") are bound unto The Oriental Insurance Company Limited (hereinafter called "the Purchaser") in the sum of Rupees _____ for which payment well and truly to be made to the said Purchaser, the Bank binds itself, its successors and assigns by these presents. Sealed with the Common Seal of the said Bank this _____ day of _____ 2015.

The Conditions of this obligation are:

If the Bidder withdraws his bid during the period of bid validity specified by the Bidder in the bid; or

If the Bidder, having been notified of the acceptance of its bid by the Purchaser during the period of bid validity

i. fails or refuses to execute the Contract Form, if required; or

ii. fails or refuses to furnish the Performance Security, in accordance with the instructions to Bidder.

We undertake to pay to the Purchaser up to the above amount upon receipt of its first written demand, without the Purchaser having to substantiate its demand, provided that in its demand the Purchaser will note that the amount claimed by it is due to it owing to the occurrence of one or both of the two conditions, specifying the occurred condition or conditions.

This guarantee will remain in force up to and including 45 days after the period of bid validity, and any demand in respect thereof should reach the Bank not later than the above date.

Dated this.....day of.....

Place: _____

Date: Seal and signature of the Bidder

12.6 Appendix 6 : Pro forma for Performance Security

To: (Name of Purchaser)

WHEREAS..... (Name of Supplier) (Hereinafter called "the Supplier") has undertaken, in pursuance of Contract No..... dated..... 2015 to supply..... (Description of Products and Services) (Hereinafter called "the Contract").

AND WHEREAS it has been stipulated by you in the said Contract that the Supplier shall furnish you with a Bank Guarantee by a recognized Bank for the sum specified therein, as security for compliance with the Supplier's performance obligations in accordance with the Contract.

AND WHEREAS we have agreed to give the Supplier a Guarantee:

THEREFORE, WE hereby affirm that we are Guarantors and responsible to you, on behalf of the Supplier, up to a total of..... (Amount of the Guarantee in Words and Figures) and we undertake to pay you, upon your first written demand declaring the Supplier to be in default under the Contract and without cavil or argument, any sum or sums within the limit of ..... (Amount of Guarantee) as aforesaid, without your needing to prove or to show grounds or reasons for your demand or the sum specified therein.

This guarantee is valid until the .....day of.....

Signature and Seal of Guarantors (Supplier's Bank)
.....
Date.....
Address.....

12.7 Appendix 7 : OEM's Authorization Form

Date: dd/mm/yyyy

To

The Deputy General Manager
Information Technology Department,
The Oriental Insurance Company Limited,
2nd Floor, Head Office, "Oriental House",
A-25/27, Asaf Ali Road,
New Delhi - 110 002

Reference: Tender No. OICL/HO/ITD/TECH-REFRESH/2015/01 Dated 28th August 2015

Sir,

We _____, (name and address of the 'manufacturer / developers') who are established and reputed 'manufacturers / developers' of _____ having factories at _____ (addresses of locations) do hereby authorize M/s _____ (name and address of the Bidder) to bid, negotiate and conclude the contract with OICL against the above mentioned tender for the proposed hardware / software manufactured/developed/customized by us.

We hereby extend our guarantee and warranty as per terms and conditions of the RFP and the contract for the hardware / software and services offered for supply against this RFP by the above-mentioned Bidder, and will extend full support for a period of 6 years.

Yours faithfully,

For and on behalf of M/s _____*(Name of the manufacturer)*

Signature _____

Name _____

Designation _____

Address _____

Date _____

Company Seal

Note: This letter of authority should be on the letterhead of the concerned manufacturer and should be signed by Authorized Signatory

12.8 Appendix 8 : Statement of No Deviation from Tender Terms and Conditions

To

The Deputy General Manager
Information Technology Department
The Oriental Insurance Company Limited
2nd Floor, Head Office, "Oriental House"
A-25/27, Asaf Ali Road
New Delhi - 110 002

Reference: Tender No. OICL/HO/ITD/TECH-REFRESH/2015/01 Dated 28th August 2015

Sir,

There are no deviations (null deviations) from the terms and conditions of the tender. All the terms and conditions of the tender are acceptable to us.

Yours faithfully,

For and on behalf of M/s _____*(Name of the manufacturer)*

Signature _____

Name _____

Designation _____

Address _____

Date _____

Company Seal

13. Annexures

This Page is Intentionally Left Blank

13.1 Annexure 1 : Technical Specifications

13.1.1 Enterprise Storage System

S.N.	Minimum Technical Specifications	Compliance (Yes/No)	Reference in enclosed Data Sheet
1	The Proposed Storage system should be Enterprise Class and of latest generation. Storage System should have support for FC, CIFS, and NFS Protocols.		
2	The proposed storage should support 400GB or higher SSD Drives / Enterprise Flash Drives, 900 GB or higher 10K RPM SAS Drives and 4 TB or higher NL-SAS or SATA Drives.		
3	The proposed system should support RAID 1/10,5,6.		
4	The proposed Storage Systems should be supplied with following usable capacity: 20 TB usable capacity in RAID 5 using 400 GB or higher SSD / Enterprise Flash Drives 240 TB usable capacity in RAID 5 using 900 GB or higher 10K RPM SAS drives. 140 TB usable capacity in RAID 6 or equivalent using 4 TB 7.2K RPM NL-SAS / SATA Drives.		
5	The Storage System should be scalable to at least 1500 Drives in future.		
6	The supported disks should be dual ported with minimum 6Gbps or higher full-duplex data transfer capability		
7	Storage System should support multiple Hot Spares. One Hot spare disk should be provided for every 30 Disk Drives.		
8	The Storage Systems should be supplied with minimum 512 GB Cache across storage controllers scalable to minimum 1TB. (Cache should not be configured in the form of SSDs.) NAS Gateways (If required) should be proposed in high availability mode with full redundancy and have separate memory.		
9	The storage should have minimum 512 Gbps FC bandwidth using 16 Gbps ports and 80GigE bandwidth for host connectivity.		
10	Storage should have with minimum 384 Gbps SAS Backend Disk Connectivity across storage controllers with native 6Gbps SAS backends.		
11	The storage should be with No Single Point of Failure (NSPOF) with redundant and hot swappable components. The proposed storage must support non-disruptive replacement of hardware components.		
12	The storage must provide non-disruptive firmware/micro code upgrade, device reallocation and configuration changes.		
13	The storage system should have support for multi-path configuration for redundant path to connected hosts. Any Licenses required for this should be provided with Storage.		
14	The storage should have protection of cache data during a power down either scheduled or unexpected power outage by battery backup for at least 72 hours OR by de-staging the data in cache to non-volatile disk / flash memory.		

Page **82** of **155**

15	The storage should support Virtual/Thin provisioning. Licences should be provided for the supplied capacity.		
16	The storage should support dynamic LUN expansion/ concatenation while LUN is mounted on the host.		
17	The storage should support data tiering between different storage tiers namely SSD and SAS/ SATA/NL-SAS within the same storage array. Licences should be provided for the supplied capacity.		
18	The storage should be able to generate audit logs.		
19	The storage should have LUN masking or equivalent feature to prevent access of a LUN from unauthorized Hosts.		
20	The storage should support multiple operating systems such as Windows, Unix, Linux, etc.		
21	The storage should support clustering solutions such as Microsoft cluster, SUN Solaris cluster, Linux cluster etc.		
22	The storage should have integration with major Database like Oracle, MSSQL, My- SQL, DB2 etc. to take application consistent copies when doing replication.		
23	Easy to use GUI based and web enabled administration interface for configuration, storage management. Storage management alerting, and reporting tools also should be bundled with the storage.		
24	**Local copy features**		
A	The storage should support local copy of single source device. Both snapshot and clones (full copy) should be supported		
B	Licences for clone should be supplied for the 80 TB of capacity.		
C	Licences for snapshot should be supplied for the 20 TB of capacity.		
25	**Remote Replication features**		
A	Offered storage system should be configured with Storage based Replication.		
B	The proposed storage should be able to utilise the FC-IP routers (Specifications mentioned in this RFP, which will be shared with existing EMC SRDF Replication) for replication of FC volumes, or else it should support IP Port based replication (In case of using IP Port based replication, 4 nos. of 10GigE IP should be additionally configured across storage controllers.) All necessary licenses should be supplied for proper functioning of the setup.		
C	Replication Licence for 40 TB of capacity should be configured for Asynchronous Replication.		
26	The Power and cooling requirements of the configuration should be submitted along with technical document		
27	Storage should be proposed with Rack of same OEM.		
28	OEM of the offered product should be listed in Leader Quadrant of Gartner “Magic Quadrant for General-Purpose Disk Arrays Published in 2014”.		

13.1.2 SAN Switch

S.N.	Minimum Technical Specifications	Compliance (Yes/ No)	Reference in enclosed Data Sheet
1	Non-blocking architecture with 96 ports in a single domain concurrently active at 16 Gbit/sec full duplex with no oversubscription. The base switch should be configured with 96 ports.		
2	All the ports should provide auto-sensing 2, 4, 8, and 16 Gbit/sec capabilities for backward compatibility using appropriate SFPs		
3	The switch shall support different port types such as , F_Port, M_Port (Mirror Port) or Equivalent, and E_Port; self-discovery based on switch type (U_Port or Auto mode Port)		
4	The switch should be rack mountable and be supplied with proper rack mount kit to mount in a standard 2U rack.		
5	Non-disruptive Microcode/ firmware Upgrades and hot code activation.		
6	The switch shall provide minimum Aggregate bandwidth of 1.536 Tb/sec (96 ports × 16 Gbit/sec (data rate) end to end)		
7	Should support Quality of Service (QoS) to help optimize application performance in consolidated, virtual environments. It should be possible to define high, medium and low priority QOS zones to expedite high priority traffic.		
8	The Switch should be configured with the Zoning and ISL Licenses, should support frame based ISL trunking		
9	The switch shall be able to support ISL trunk up to 128 Gbit/sec between a pair of switches for optimal bandwidth utilization and load balancing.		
10	Support for web based management and should also support CLI.		
11	The switch shall support advanced zoning (Port/WWN based zoning) and ACL to simplify administration and significantly increase control over data access.		
12	It shall be possible to configure the switches with alerts based on threshold values for temperature, fan status, Power supply status, port status.		
13	Switch shall support POST and online/offline diagnostics, including environmental monitoring, non-disruptive daemon restart, FC ping and Pathinfo (FC trace route), port mirroring (SPAN port).		
14	Should provide enterprise-class availability features such as redundant and hot pluggable components.		
15	Should have Front-to-back / Back-to-front airflow		
16	The switch should support Inflight Encryption		
17	The switch should be provided with the required LWL/ELWL SFPs and licenses to connect to NLDC over dark Fibre or XWDM		
18	The switch should support Forward Error Correction and Dynamic Fabric Provisioning		
19	LC-LC Cables (48 x 10 meter & 48 x 15 meter)		

13.1.3 FC-IP Routers

S.N.	Minimum Technical Specifications	Compliance (Yes/No)	Reference in enclosed Data Sheet
1	Shall have non-blocking switching fabric and wired rate throughput on all interfaces. All FC ports should be minimum 8 Gbps. Should auto negotiate with 8/4/2 G		
2	Switch shall have atleast 4 FC ports scalable to 16 FC ports and minimum 2 x 1 G ports		
3	The switch must support FCIP/FC/FCR protocols and support both FC as well as FCIP Trunking.		
4	It shall be possible to trunk maximum 8 ports/ links together. Should have no limit on the number of Trunks that can be configured.		
5	The FCIP Switch must support the non-disruptive E-port fabric connection to fibre channel switches.		
6	The FCIP Switch must support the following fibre channel port types: • F-Port • FL-Port • E- Port/VE Port • M- Port or Equivalent • U- Port / AUTO mode port(Self Discovery based on Switch type).		
7	The FCIP Switch shall have the capability to replicate the Data using any of the following replication software's like EMC SRDF, HDS True copy, PPRC, HP Continuous access, etc.		
8	The FCIP Switch must support advanced SAN extension capabilities: a. Fast Write SCSI for FCIP and FC b. Hardware based compression c. Tape Pipelining (Read & Write) d. Remote SAN connectivity without merging fabrics		
9	The FCIP Switch should be capable of supporting Compression on each port for FC-IP functionality and IPsec encryption without any additional software license		
10	The FCIP switch should support minimum 3 multiple virtual channels per GE port		
11	Switch should have in-built diagnostics, power on self-test, command level diagnostics, online and offline diagnostics.		
12	Non-disruptive Microcode/ firmware Upgrades and hot code activation		
13	The Switch should have redundant fan and power supplies		
14	It shall be possible to configure the switch with alerts based on threshold values for temperature, fan status, Power supply status, port status.		

13.1.4 Tape Library

S.N.	Parameter	Minimum Technical Specifications	Compliance (Yes/ No)	Reference in Enclosed Datasheet
1	Tape Drives	Tape Library shall be offered with Minimum of 8 LTO6 FC tape drives and shall be scalable to 16 numbers of LTO-6 Drives within the same Library.		
2	Cartridge Slots	Tape Library shall be offered with minimum 200 Cartridge slots and shall be scalable to 300 slots		
3	Tape Drive Architecture	Offered LTO6 drive in the Library shall conform to the Continuous and Data rate matching technique for higher reliability.		
4	Cartridges	Tape Library shall be offered with 200 Tape Cartridges & 20 Cleaning Cartridges with barcodes.		
5	Speed	Offered LTO6 drive shall support 160MB/sec in Native mode and 400MB/sec in 2.5:1 Compressed mode.		
6	Connectivity	Offered Tape Library shall provide 8Gbps native FC connectivity to SAN switches.		
7	Management	Tape Library shall provide web based remote management.		
8	Barcode Reader	Tape library shall support Barcode reader or equivalent technology.		
9	Other Features	1. Tape Library shall have GUI Panel 2. Tape Library shall be supplied with software which can predict and prevent failures through early warning and shall also suggest the required service action. 3. Offered Software shall also have the capability to determine when to retire the tape cartridges and what compression ratio is being achieved		

13.1.5 Disk Based Backup Appliance

S.N.	Minimum Technical Specifications	Compliance (Yes/ No)	Reference in Enclosed Datasheet
1	The Proposed Disk based backup appliance should be supplied with: - 100 TB of Usable capacity Using SATA / NL-SAS Drives in RAID 6 or equivalent. - 4 x 8 Gbps FC & 2 x 10 Gbps LAN Connectivity - Scalable to 200 TB of Usable capacity		
2	Offered device should have integrated de-duplication license in a low bandwidth mode so that only unique – Non Duplicated data flows to remote location.		
3	Offered disk based backup device shall also support encryption functionality		
4	Offered device should support rated write performance of at-least 8 TB per hour		
5	Appliance should be offered with hot spare disks in atleast 15:1 ratio.		
6	Data replication should be enabled on the offered solution for 20 TB.		

13.1.6 Backup Software

S.N.	Minimum Technical Specifications	Compliance (Yes/No)
1	Should be available on various OS platforms such as Windows, Linux and UNIX platforms and be capable of supporting backup / restores from various platforms including Oracle Solaris, HP-UX, IBM AIX, Linux, NetWare.	
2	Software should have full command line support on above mention operating systems.	
3	The backup software should be able to encrypt the backed up data using 256-bit AES encryption on the backup client and should not demand for additional license, any such license if needed should be quoted for the total number of backup clients asked for.	
4	Must support wizard-driven configuration and modifications for backups and devices	
5	The backup software should provide comprehensive device reporting and handling.	
6	Should have cross platform Domain Architecture for User management and should also have role based User management and access control for multitenant environments.	
7	Should have firewall support.	
8	Must support de-duplicated backup and recovery for Microsoft Hyper-V using VSS at the host (parent partition) to protect both the host and guest (child partition).	
9	Should have in-built scheduling system and also support check-point restart able backups.	
10	Should support backups for clustered servers and support industry popular clusters like Sun cluster, HP service guard, HACMP i.e. should have the ability to backup data from clustered servers from the virtual client, backing up data only once and giving consistent backup in case of failover of nodes.	
11	Must support backup / recovery of raw SCSI volumes	
12	Backup methodology should be LAN Free. Pricing of the software should not to be dependent on the number of CPUs of the client machines. Upgrading the client machines and increasing CPU should not have any commercial implications in terms of renewing licenses or buying additional licenses.	
13	Should support advanced backup to disk backups where backups and restores from the backup media (disk in this case) can be done simultaneously.	
14	Should support NDMP multiplexing of NDMP and non NDMP data to the same tape and should also support NDMP backup to disk.	
15	The backup software should support backup and restore of NDMP data to media server attached tape/VTL.	

16	Should integrate with third party VTL which has data deduplication capabilities.	
17	Must support source capacity based licensing which should have no impact incase if the number of processor are increased in the server being backed up.	
18	Quoted Backup software must support more than 1 worker/storage/media server which works as worker to receive backup data from clients and write data to tape.	
19	Must support Hardware and storage array based snapshot backup for off host zero downtime and zero load on the primary backup client.	
20	The backup software should support data movement directly from the backup client to the disk target without passing through the backup server.	
21	Software to be licensed for 100 TB of data.	
22	The proposed solution should be positioned as a Leader in the latest Gartner's Magic Quadrant for Enterprise Backup Software.	

13.1.7 Blade Chassis

S.N.	Parameter	Minimum Technical Specifications	Compliance (Yes/ No)	Reference in enclosed Data Sheet
1	Form Factor	Chassis solution be Rack Mountable. Offered solution should support minimum 14 Blade Servers from day one.		
2	Management Module	The blade chassis should be configured with Hot swap IP based KVM Switch Module for Management.		
3	Mid-plane	Should have passive mid-plane architecture		
4	I/O Switch Modules	The blade chassis should have redundant I/O Switch Modules.		
5	Ethernet & SAN Connectivity	Sufficient number of 10G based converged redundant modules for LAN and SAN connectivity should be configured.		
		For LAN uplink, solution should provide 8 numbers of 1G RJ45 SFP and 8 numbers of 10G SR SFP along with 15m LC-LC Cable.		
		For SAN uplink, solution should provide 8 numbers of 8 Gbps FC/FCoE uplinks along with 15m LC-LC Cable.		
6	Power Modules	Chassis should be configured with all the power supplies and should support N+N as well as N+1 configuration.		
7	Cooling Modules	Hot swap and redundant cooling fans. All fans should be fully populated		
8	DVD Drive	The chassis solution should have minimum 1 DVD ROM (Internal / External) which can be used by all the blade servers or should support virtual media to mount DVD/CD from remote system.		
9	System Management	System Management and deployment tools to aid configuring the Blade Servers and OS Deployment should be provided		
10	Power & Cooling Requirement	The Power and cooling requirements of the configuration should be submitted along with technical document		
11	OEM Eligibility	OEM of the offered product should be listed in Leaders or Challengers quadrant of Gartner “Magic Quadrant for Modular Servers Published in 2015”.		

13.1.8 Backup Server

S.N.	Parameters	Minimum Technical Specifications	Compliance (Yes/ No)	Reference in enclosed Data Sheet
1	Processor	2 * Intel Xeon E5-2600v3 12 Core or better Processor with minimum 2.6 GHz		
2	Chipset	Latest compatible chipset supporting above processor		
3	Memory	As per Solution (Minimum 8 GB per core)		
4	HDD	As per Solution (Minimum 2 * 900 GB 10K SAS HDD hot swappable system disk with mirroring using integrated RAID 0,1 on internal disks)		
5	Ethernet & SAN Connectivity	The Blade server should be configured with Converged Network Adapter of atleast 36 Gbps which aggregates both the Ethernet (2 x 10G) and FC (2 x 8G) bandwidth.		
6	Management Features	Managing servers in Physical, Local and Remote environments and should be able to monitor all systems components (BIOS, HBA's, NICs, and CNA's).		
7	Security Features	Power-on password, administrator password.		
8	USB Port	Blade server should have one USB Port.		
9	Operating System	As per Solution		
10	Power & Cooling Requirement	The Power and cooling requirements of the configuration should be submitted along with technical document		
11	Form Factor	Blade		

13.1.9 NOC & HRMS Reporting Servers

S.N.	Parameters	Minimum Technical Specifications	Compliance (Yes/ No)	Reference in enclosed Data Sheet
1	Processor	2 * 8 Core Intel Xeon Latest E5-2600 v3 Processor with minimum 2.6 GHz		
2	Chipset	Latest compatible chipset supporting above processor		
3	Memory	64 GB RAM		
4	HDD	2 * 900 GB 10K SAS HDD hot swappable system disk with mirroring using integrated RAID 0,1 on internal disks.		
5	Ethernet & SAN Connectivity	The Blade server should be configured with Converged Network Adapter of atleast 36 Gbps which aggregates both the Ethernet (2 x 10G) and FC (2 x 8G) bandwidth.		
6	Management Features	Managing servers in Physical, Local and Remote environments and should be able to monitor all systems components (BIOS, HBA's, NICs, and CNA's).		
7	Security Features	Power-on password, administrator password.		
8	USB Port	Blade server should have one USB Port.		
9	Operating System	Microsoft Windows 2012 Standard Edition		
10	Power & Cooling Requirement	The Power and cooling requirements of the configuration should be submitted along with technical document		
11	Form Factor	Blade		

13.1.10 Mail Messaging Servers

S.N.	Parameters	Minimum Technical Specifications	Compliance (Yes/ No)	Reference in enclosed Data Sheet
1	Processor	2 * Intel Xeon Latest E5 or E7 Series Processor		
2	Chipset	Latest compatible chipset supporting above processor		
3	Memory	As per Solution (Minimum 8 GB per core)		
4	HDD	As per Solution (Minimum 2 * 900 GB 10K SAS HDD hot swappable system disk with mirroring using integrated RAID 0,1 on internal disks)		
5	Ethernet & SAN Connectivity	The Blade server should be configured with Converged Network Adapter of atleast 36 Gbps which aggregates both the Ethernet (2 x 10G) and FC (2 x 8G) bandwidth.		
6	Management Features	Managing servers in Physical, Local and Remote environments and should be able to monitor all systems components (BIOS, HBA's, NICs, and CNA's).		
7	Security Features	Power-on password, administrator password.		
8	USB Port	Blade server should have one USB Port.		
9	Operating System	As per Solution		
10	Power & Cooling Requirement	The Power and cooling requirements of the configuration should be submitted along with technical document		
11	Form Factor	Blade		

13.1.11 DR Management and Other Servers

S.N.	Parameters	Minimum Technical Specifications	Compliance (Yes/ No)	Reference in enclosed Data Sheet
1	Processor	2 * Intel Xeon Latest E5 2600 v3 Series Processor		
2	Chipset	Latest compatible chipset supporting above processor		
3	Memory	As per Solution (Minimum 8 GB per core)		
4	HDD	As per Solution (Minimum 2 * 900 GB 10K SAS HDD hot swappable system disk with mirroring using integrated RAID 0,1 on internal disks)		
5	Ethernet & SAN Connectivity	The Blade server should be configured with Converged Network Adapter of atleast 36 Gbps which aggregates both the Ethernet (2 x 10G) and FC (2 x 8G) bandwidth.		
6	Management Features	Managing servers in Physical, Local and Remote environments and should be able to monitor all systems components (BIOS, HBA's, NICs, and CNA's).		
7	Security Features	Power-on password, administrator password.		
8	USB Port	Blade server should have one USB Port.		
9	Operating System	As per Solution		
10	Power & Cooling Requirement	The Power and cooling requirements of the configuration should be submitted along with technical document		
11	Form Factor	Blade		

13.1.12 Server - CTA

S.N.	Parameters	Minimum Technical Specifications	Compliance (Yes/ No)	Reference in enclosed Data Sheet
1	Processor	2 * 8 Core Intel Xeon Latest E5-2600 v3 Processor with minimum 2.6 GHz		
2	Chipset	Latest compatible chipset supporting above processor		
3	Memory	64 GB RAM		
4	HDD	6 * 600 GB 10K SAS HDD with RAID-5		
5	Ethernet Connectivity	Server should be configured with 2 * 10G SFP+ and 4 * 1G Ethernet ports		
6	SAN Connectivity	Server should be configured with 2 Number of 16G FC ports		
7	Management Features	Managing servers in Physical, Local and Remote environments and should be able to monitor all systems components (BIOS, HBA's, NICs).		
8	Security Features	Power-on password, administrator password.		
9	USB Port	Server should have one USB Port.		
10	Operating System	Oracle Linux 6.3		
11	Power & Cooling Requirement	The Power and cooling requirements of the configuration should be submitted along with technical document		
12	Form Factor	Rack		

13.1.13 Server - OEM

S.N.	Parameters	Minimum Technical Specifications	Compliance (Yes/ No)	Reference in enclosed Data Sheet
1	Processor	2 * 8 Core Intel Xeon Latest E5-2600 v3 Processor with minimum 2.6 GHz		
2	Chipset	Latest compatible chipset supporting above processor		
3	Memory	64 GB RAM		
4	HDD	6 * 600 GB 10K SAS HDD with RAID-5		
5	Ethernet Connectivity	Server should be configured with 2 * 10G SFP+ and 4 * 1G Ethernet ports		
6	SAN Connectivity	Server should be configured with 2 Number of 16G FC ports		
7	Management Features	Managing servers in Physical, Local and Remote environments and should be able to monitor all systems components (BIOS, HBA's, NICs).		
8	Security Features	Power-on password, administrator password.		
9	USB Port	Server should have one USB Port.		
10	Operating System	RHEL Latest Version (1-4 Guest)		
11	Power & Cooling Requirement	The Power and cooling requirements of the configuration should be submitted along with technical document		
12	Form Factor	Rack		

13.1.14 Core Switch

S.N.	Parameter	Minimum Technical Specifications	Compliance (Yes/No)	Reference in enclosed Data Sheet
1	Availability and Redundancy	There should not be any single point of failure in the switch. All the main components like CPU module, switching fabric, support module, power supplies and fans etc. should be in redundant configuration. Components, like modules/power supplies/fan tray should be Hot Swappable		
2	Availability and Redundancy	The switch should have redundant CPU's working in an active-active or active-standby mode. There should not be any traffic disruption during the CPU fail-over/change-over and the fail-over time should be less than 1 sec.		
3	Availability and Redundancy	Must Have Redundancy for Power Supply and FANs to minimize unavailability of switch. Online insertion and removal (OIR) support is must for modules, Power supply and FAN.		
4	Availability and Redundancy	Stateful Switchover to ensure that in case of failure of active CPU module the redundant CPU should start switching L2/L3 traffic in less than 1 sec (in case switch has redundant CPU).		
5	Availability and Redundancy	The switch must support Hitless software upgrades (ISSU) to reduce downtime during software upgrade or downgrade.		
6	Availability and Redundancy	The switch must support Fault isolation per process and process patching to enhance the switch availability		
7	Generic	The proposed switch should have enough Memory (Flash and RAM) to hold the latest Software Release. It should support all features of switch and parameters like MAC Address Table, IP Routing Tables, VLANs etc.at their peak values as claimed in the Data Sheets of the Switch.		
8	Generic	The Switch should have a Truly Distributed Architecture. All Interface Modules should have all the resources for switching and Routing and should offer True Local Switching (Intra-Module and Inter-Module).		
9	Generic	Version of software for supplied switch should be latest release with necessary licenses to support all required features		
10	Generic	IEEE 802.1D Bridging and Spanning Tree		
11	Generic	IEEE 802.1p QoS/CoS		
12	Generic	IEEE 802.1Q VLAN Tagging		
13	Generic	IEEE 802.1w Rapid Spanning Tree		
14	Generic	IEEE 802.1s Multiple Spanning Tree Protocol		
15	Generic	IEEE 802.1AB Link Layer Discovery Protocol		

16	Generic	IEEE 802.3ad Link Aggregation with LACP		
17	Generic	IEEE 802.3x Flow Control		
18	Generic	IEEE 802.3ab 1000BASE-T		
19	Generic	IEEE 802.3z Gigabit Ethernet		
20	Generic	IEEE 802.3ae 10 Gigabit Ethernet		
21	Generic	IEEE 802.3ba 40 Gigabit Ethernet		
22	Generic	RFC 2460 IPv6		
23	Generic	RFC 2461 Neighbor Discovery for IPv6		
24	Generic	RFC 2462 IPv6 Stateless Address Auto configuration		
25	Generic	RFC 2463 ICMPv6		
26	Layer 2 features	Should support Ingress/Egress Queuing.		
27	Layer 2 features	Should support QoS scheduling with queues supported in hardware		
28	Layer 2 features	Should support upto 4 queues per port		
29	Layer 2 features	Should support ACL based traffic classification		
30	Layer 2 features	Should Support IGMP v1, v2 , v3, IGMP Snooping		
31	Layer 2 features	Should support Industry Standard Port/Link Aggregation for All Ports. Also Cross Module Link aggregation should be supported		
32	Layer 2 features	Jumbo Frames support up to 9K Bytes on Gigabit / 10 G Ports		
33	Layer 2 features	Support for broadcast, multicast and unknown unicast storm control to prevent degradation of switch performance from faulty end stations		
34	Layer 2 features	Should support port, subnet based 802.1Q VLANs. The switch should support 4094 vlans. The switch must support Private VLAN or equivalent.		
35	Layer 2 features	The switch should support 160,000 no. of MAC addresses.		
36	Layer 2 features	The switch should support more than 128 nos. of Link Aggregation Group per switch.		
37	Layer 2 features	Switch must support multi chassis link aggregation feature and work with any downstream other OEM switch, server from various Bidders		
38	Layer 3 features	Should have support routing protocol IP v4 - Static routing, OSPF v2, BGPv4, IS-IS and IP v6 - BGP, OSPF v3. The switch must support Bidirectional Forwarding detection on OSPF and BGP.		
39	Layer 3 features	Switch must support IP v4 - VRRP and IP v6 - VRRP It must also support DHCP Relay V4 and V6.		
40	Layer 3 features	Switch should support VRF - Lite and VRF Route leaking functionality. The switch should support upto 1000 VRF instances.		

41	Layer 3 features	Should support minimum 64k Route entries for IPv4 and IPv6 routes.		
42	Layer 3 features	Should support H/W based IPv4 and IPv6 Multicasting		
43	Layer 3 features	Should support Protocol Independent Multicast - Sparse Mode and PIM - ASM/SSM for IPv4 and MSDP for IP v6. It should also support Anycast Routing Protocol (Anycast RP).		
44	Layer 3 features	Switch should support atleast 2K Multicast route		
45	Management and Operation	Switch should be manageable through NMS on per port/switch basis with common interface for all manageable devices on the network. Should Support SNMP, RMON/RMON-II, SSH, telnet, web management through network management software.		
46	Management and Operation	Should support port mirroring feature for monitoring network traffic of a particular port/VLAN/group of ports/entire switch. The switch should support port mirroring Session		
47	Management and Operation	Switch should support Syslog, SSHv2, Telnet, OOB Management port, Console Port.		
48	Management and Operation	The switch should support configuration verification and roll-back.		
49	Management and Operation	The switch should support SNMP v1,v2c and V3		
50	Performance & Scalability	Chassis based Multilayer Switch with sufficient modules/line cards to fit required transceivers/UTP ports. Chassis shall have minimum 8 payload slots.		
51	Performance & Scalability	Switch must have minimum 48 nos. of 10 G Base-T ports, minimum 48 no. of 10 Gig SFP+ ports loaded with 12 nos. of SFP-SR MM fibred modules and additional 8 nos. of 40 Gig QSFP ports, loaded with QSFP transceiver modules.		
52	Performance & Scalability	Switching system shall have minimum throughput of 2.5 Tbps full duplex per slot, and scalable to 10 Tbps full-duplex in future without chassis upgrade.		
53	Performance & Scalability	Switching system should be scalable to additional 288 no. of 10 Gig and 24 nos. of 40 Gig Ports, for future requirements of inter-device uplinks and server connectivity.		
54	Performance & Scalability	The 40G ports on the switch can be usable either for an uplink connectivity to the core switch or for downlink connectivity to the 40G server.		
55	Performance & Scalability	The Switch should support non-blocking Layer 2 switching and Layer 3 routing.		
56	Performance & Scalability	The Backplane should be 100% Passive. Preferably back plane free design to optimize the airflow and power consumption.		
57	Performance & Scalability	The switch must support 100 Gig line cards for future requirements and scalability.		

58	Security	Should support Standard and Extended ACLs		
59	Security	Should support various type of ACLs like MAC Based, Port based, Vlan Based and routed ACLs.		
60	Security	Should support integrated security features like DHCP snooping with option-82, Dynamic Arp Inspection, IP Source guard and uRPF (unicast Reverse path forwarding)		
61	Security	Should Support MAC Address Filtering based on source and destination address		
62	Security	Should support AAA, with CHAP, PAP, CHAP. It must support LDAP, RADIUS and TACACS+ protocol as well.		
63	Security	The switch must support Role Based access control (RBAC) for L1, L2 and L3/Administrators.		
64	Security	The switch should support control plane policing to filter the unwanted traffic to fill up the CPU queues.		
65	Security	The switch should support ingress ACLs. It should support Security and QOS ACL's.		
66	Regulatory compliance	Products should comply with CE Markings according to directives 2004/108/EC or 2006/95/EC		
67	Safety	• UL 60950-1 Second Edition		
		• CAN/CSA-C22.2 No. 60950-1 Second Edition		
		• EN 60950-1 Second Edition		
		• IEC 60950-1 Second Edition		
		• AS/NZS 60950-1		
68	EMC: Emissions	• 47CFR Part 15 (CFR 47) Class A		
		• AS/NZS CISPR22 Class A		
		• CISPR22 Class A		
		• EN55022 Class A		
		• ICES003 Class A		
		• VCCI Class A		
		• EN61000-3-2		
		• EN61000-3-3		
69	EMC: Immunity	• EN55024		
70	RoHS	RoHS compliant		

13.1.15 DMZ Switch

S.N.	Parameter	Minimum Technical Specification	Compliance (Yes/No)	Reference in enclosed Data Sheet
1	Availability and Redundancy	Switch must provide front to back airflow and also has an option of reverse airflow if required.		
2	Availability and Redundancy	Network infrastructure should run at an ambient temperature of ~27ºC without impact to MTBF.		
3	Availability and Redundancy	Must have Redundant Power Supply Units (PSUs), Hot-swappable, field-replaceable power supplies, 1:1 power redundancy.		
4	Availability and Redundancy	Must have N:1 fan module redundancy.		
5	Availability and Redundancy	All components (including elements such as I/O cards, Expansion Module, power supplies and fans) must be hot swappable with zero disruption to traffic forwarding (Unicast or multicast).		
6	Availability and Redundancy	In the event of a PSU failure, a single power supply Must be able to support the network device.		
7	Generic	The proposed switch solution can be either a fixed configuration switch or a modular switch or combination of switches. The proposed switch size should not be more than 13 Rack Units.		
8	Generic	The proposed switch should support FCOE and DCB features or it should be in roadmap.		
9	Generic	Must support Gigabit Ethernet (IEEE 802.3z, 802.3ab) and Ten Gigabit Ethernet (IEEE 802.3ae)		
10	Generic	Must support IEEE 802.1d - Spanning-Tree Protocol		
11	Generic	Must support IEEE 802.1w - Rapid Spanning Tree		
12	Generic	Must support IEEE 802.1s - Multiple Spanning Tree Protocol		
13	Generic	Must support IEEE 802.3ad - Link Aggregation Control Protocol (LACP)		
14	Generic	The proposed switch should support GRE (Generic routing encapsulation) Tunnel		

15	Generic	Must support IEEE 802.1ab - Link Layer Discovery Protocol (LLDP)		
16	Generic	Must support IEEE 802.3x Flow Control		
17	Layer 2 features	Must support link aggregation across multi chassis.		
18	Layer 2 features	Must have Layer 2 IEEE 802.1p		
19	Layer 2 features	Must have 4 hardware queues per port with per port QoS configuration		
20	Layer 2 features	Must have Modular QoS classification compliance		
21	Layer 2 features	Must have per port virtual output queuing		
22	Layer 2 features	Must have link aggregation support allowing upto 8 ports per link aggregation group		
23	Layer 2 features	Must support Jumbo Frame Size (9k)		
24	Layer 2 features	Must have Per-Port QoS configuration		
25	Layer 2 features	Must have CoS Trust and CoS-based egress queuing		
26	Layer 2 features	Must have Egress strict-priority queuing		
27	Layer 2 features	Must have ACL-based QoS classification (Layers 2, 3, and 4)		
28	Layer 3 features	Should support routing protocol IP v4 - Static routing, OSPF v2, BGPv4, IS-IS and IP v6 - BGP, OSPF v3. The switch must support Bidirectional Forwarding detection on OSPF and BGP.		
29	Layer 3 features	Must support Protocol Independent Multicast Version 2 (PIMv2) sparse mode, Source Specific Multicast (SSM), Multicast Source Discovery Protocol (MSDP), and Internet Group Management Protocol Versions 2, and 3 (IGMP v2, and v3)		
30	Layer 3 features	Support for up to 8000 multicast routes.		
31	Layer 3 features	Support for 1000 VRF entries		
32	Layer 3 features	Virtual Route Forwarding (VRF) or equivalent: VRF-lite (IP VPN); VRF-aware unicast; and BGP-, OSPF-, and VRF-aware multicast		

33	Layer 3 features	Must support 8 way equal-cost multipathing (ECMP)		
34	Management & Operation	Must provide management using 10/100/1000-Mbps out of band management interface and console ports		
35	Management & Operation	Must support In-band switch management		
36	Management & Operation	Must have Configuration synchronization & Configuration rollback		
37	Management & Operation	Must support Secure Shell Version 2 (SSHv2), Telnet & SNMPv1, v2, and v3		
38	Management & Operation	Must support AAA, AAA with RBAC, Radius, TACACS+ for user authentication		
39	Management & Operation	Must have Advanced Encryption Standard (AES) for management traffic		
40	Management & Operation	Must provide Comprehensive bootup diagnostic tests		
41	Management & Operation	Must support port mirroring on physical, Port Channel and VLAN interfaces		
42	Management & Operation	Must have Embedded packet analyser like ethereal		
43	Performance & Scalability	Must have minimum 48 x 1/10 G SFP+ and 6 X 40 G QSFP ports. with minimum 16 nos. of 1G modules, 16 nos. of 1000 Base-T modules and 16 no. of 10 Gig-SR with MM fibre modules		
44	Performance & Scalability	Must have Layer 2 hardware forwarding of 1.4 Tbps or higher.		
45	Performance & Scalability	Must have additional scalability for 6x40 G ports for future use.		
46	Performance & Scalability	The 40G ports on the switch should be usable either for uplink connectivity to the core switch or for downlink connectivity to the 40G server.		
47	Performance & Scalability	Must have latency of less than 2 micro-seconds.		
48	Performance & Scalability	Must have Line-rate traffic throughput on all ports at Layer 2 and Layer 3		
49	Performance & Scalability	The proposed switch Must support minimum 16000 IPV4 routes and 8000 IPV6 routes		

50	Performance & Scalability	Must support minimum 96,000 MAC address table entries.		
51	Security	Must support multiple privilege levels for remote access (e.g. console or telnet access)		
52	Security	Must support 4000 Ingress ACLs (Standard & Extended) on Ethernet and virtual Ethernet ports		
53	Security	Must support Standard and extended Layer 2 ACLs: MAC addresses, protocol type, etc.		
54	Security	Must support Standard and extended Layer 3 to 4 ACLs: IPv4 and v6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP), etc.		
55	Security	Must support VLAN based ACLs (VACLs) and Port-Based ACLs (PACLs)		
56	Security	Must support ACL logging and statistics		
57	Security	Must support Storm control (unicast, multicast, and broadcast)		
58	Regulatory compliance	Safety - ● UL 60950-1 Second Edition ● CAN/CSA-C22.2 No. 60950-1 Second Edition ● EN 60950-1 Second Edition ● IEC 60950-1 Second Edition ● AS/NZS 60950-1		
59	Regulatory compliance	EMC: Emissions - ● 47CFR Part 15 (CFR 47) Class A ● AS/NZS CISPR22 Class A ● CISPR22 Class A ● EN55022 Class A ● ICES003 Class A ● VCCI Class A ● EN61000-3-2 ● EN61000-3-3		
60	Regulatory compliance	EMC: Immunity - ● EN55024		

13.1.16 Distribution Switch

S.N.	Criteria	Minimum Technical Specification	Compliance (Yes/No)	Reference in enclosed Data Sheet
1	Availability and Redundancy	Switch must provide front to back airflow and also has an option of reverse airflow if required.		
2	Availability and Redundancy	Network infrastructure should run at an ambient temperature of ~27ºC without impact to MTBF.		
3	Availability and Redundancy	Must have Redundant Power Supply Units (PSUs), Hot-swappable, field-replaceable power supplies, 1:1 power redundancy.		
4	Availability and Redundancy	Must have N:1 fan module redundancy.		
5	Availability and Redundancy	All components (including elements such as I/O cards, Expansion Module, power supplies and fans) must be hot swappable with zero disruption to traffic forwarding (Unicast or multicast).		
6	Availability and Redundancy	In the event of a PSU failure, a single power supply Must be able to support the network device.		
7	Generic	The proposed switch solution can be either a fixed configuration switch or a modular switch or combination of switches. The proposed switch size should not be more than 13 Rack Units.		
8	Generic	The proposed switch should support FCOE and DCB features or it should be in roadmap.		
9	Generic	Must support Gigabit Ethernet (IEEE 802.3z, 802.3ab) and Ten Gigabit Ethernet (IEEE 802.3ae)		
10	Generic	Must support IEEE 802.1d - Spanning-Tree Protocol		
11	Generic	Must support IEEE 802.1w - Rapid Spanning Tree		
12	Generic	Must support IEEE 802.1s - Multiple Spanning Tree Protocol		
13	Generic	Must support IEEE 802.3ad - Link Aggregation Control Protocol (LACP)		
14	Generic	The proposed switch should support GRE (Generic routing encapsulation) Tunnel		

15	Generic	Must support IEEE 802.1ab - Link Layer Discovery Protocol (LLDP)		
16	Generic	Must support IEEE 802.3x Flow Control		
17	Layer 2 features	Must support link aggregation across multi chassis.		
18	Layer 2 features	Must have Layer 2 IEEE 802.1p		
19	Layer 2 features	Must have 4 hardware queues per port with per port QoS configuration		
20	Layer 2 features	Must have Modular QoS classification compliance		
21	Layer 2 features	Must have per port virtual output queuing		
22	Layer 2 features	Must have link aggregation support allowing upto 8 ports per link aggregation group		
23	Layer 2 features	Must support Jumbo Frame Size (9k)		
24	Layer 2 features	Must have Per-Port QoS configuration		
25	Layer 2 features	Must have CoS Trust and CoS-based egress queuing		
26	Layer 2 features	Must have Egress strict-priority queuing		
27	Layer 2 features	Must have ACL-based QoS classification (Layers 2, 3, and 4)		
28	Layer 3 features	Should support routing protocol IP v4 - Static routing, OSPF v2, BGPv4, IS-IS and IP v6 - BGP, OSPF v3. The switch must support Bidirectional Forwarding detection on OSPF and BGP.		
29	Layer 3 features	Must support Protocol Independent Multicast Version 2 (PIMv2) sparse mode, Source Specific Multicast (SSM), Multicast Source Discovery Protocol (MSDP), and Internet Group Management Protocol Versions 2, and 3 (IGMP v2, and v3)		
30	Layer 3 features	Support for up to 8000 multicast routes .		
31	Layer 3 features	Support for 1000 VRF entries		
32	Layer 3 features	Virtual Route Forwarding (VRF): VRF-lite (IP VPN); VRF-aware unicast; and BGP-, OSPF-, and VRF-aware multicast		

33	Layer 3 features	Must support 8 way equal-cost multipathing (ECMP)		
34	Management & Operation	Must provide management using 10/100/1000-Mbps out of band management interface and console ports		
35	Management & Operation	Must support In-band switch management		
36	Management & Operation	Must have Configuration synchronization & Configuration rollback		
37	Management & Operation	Must support Secure Shell Version 2 (SSHv2), Telnet & SNMPv1, v2, and v3		
38	Management & Operation	Must support AAA, AAA with RBAC, Radius, TACACS+ for user authentication		
39	Management & Operation	Must have Advanced Encryption Standard (AES) for management traffic		
40	Management & Operation	Must provide Comprehensive bootup diagnostic tests		
41	Management & Operation	Must support port mirroring on physical, Port Channel and VLAN interfaces		
42	Management & Operation	Must have Embedded packet analyser like ethereal		
43	Performance & Scalability	Must have minimum 48 x 1/10 G SFP+ and 6 X 40 G QSFP ports. with minimum 8 nos. of 1G Fibre modules, 24 nos. of 1000 Base-T modules and 16 no. of 10 Gig-SR with MM fibre modules		
44	Performance & Scalability	Must have Layer 2 hardware forwarding of 1.4 Tbps or higher.		
45	Performance & Scalability	Must have additional scalability for 6x40 G ports for future use.		
46	Performance & Scalability	The 40G ports on the switch should be usable either for uplink connectivity to the core switch or for downlink connectivity to the 40G server.		
47	Performance & Scalability	Must have latency of less than 2 micro-seconds.		
48	Performance & Scalability	Must have Line-rate traffic throughput on all ports at Layer 2 and Layer 3		
49	Performance & Scalability	The proposed switch Must support minimum 16000 IPV4 routes and 8000 IPV6 routes		

50	Performance & Scalability	Must support minimum 96,000 MAC address table entries.		
51	Security	Must support multiple privilege levels for remote access (e.g. console or telnet access)		
52	Security	Must support 4000 Ingress ACLs (Standard & Extended) on Ethernet and virtual Ethernet ports		
53	Security	Must support Standard and extended Layer 2 ACLs: MAC addresses, protocol type, etc.		
54	Security	Must support Standard and extended Layer 3 to 4 ACLs: IPv4 and v6, Internet Control Message Protocol (ICMP), TCP, User Datagram Protocol (UDP), etc.		
55	Security	Must support VLAN based ACLs (VACLs) and Port-Based ACLs (PACLs)		
56	Security	Must support ACL logging and statistics		
57	Security	Must support Storm control (unicast, multicast, and broadcast)		
58	Regulatory compliance	Safety - ● UL 60950-1 Second Edition ● CAN/CSA-C22.2 No. 60950-1 Second Edition ● EN 60950-1 Second Edition ● IEC 60950-1 Second Edition ● AS/NZS 60950-1		
59	Regulatory compliance	EMC: Emissions - ● 47CFR Part 15 (CFR 47) Class A ● AS/NZS CISPR22 Class A ● CISPR22 Class A ● EN55022 Class A ● ICES003 Class A ● VCCI Class A ● EN61000-3-2 ● EN61000-3-3		
60	Regulatory compliance	EMC: Immunity - ● EN55024		

13.1.17 Core & DMZ Firewall with Integrated IPS

S.N.	Minimum Technical Specifications	Compliance (Yes/No)	Reference in enclosed Data Sheet
1	The proposed firewall should have at least 8 nos. of 10/100/1000 Base-T interfaces and 4 Nos. of 10G interfaces from day one.		
2	Proposed Firewall Should be an enterprise Firewall with modular architecture with integrated IPS and Anti-BOT solution.		
3	Should support 1,000,000 concurrent sessions for firewall		
4	Firewall should be supplied with the support for dynamic routing protocols, like RIP v2 and OSPF, OSPFv3, PBR, BGPv4, BGP for IPv6		
5	Complete firewall management solution including real-time monitoring, event logs collection, & policy enforcement should be provided.		
6	The firewall should have atleast 12 GB of Memory		
7	Firewall should support a provision to support Web 2.0, Application Control, Content Filtering features if required in future		
8	Should support AD Integration		
9	Should support IPv6.		
10	Firewall should support Stateful policy inspection. It should also have application intelligence for commonly used TCP/IP protocols like telnet, ftp etc.		
11	Firewall should have Console port and USB Ports		
12	Appliance should be supplied with minimum of 2 GB RAM/Flash.		
13	Firewall should have dedicated out of management port		
14	Should support VLAN tagging (IEEE 802.1q)		
15	Should be rack mountable and deployed for Active/Passive failover architecture. It should also support Active-Active deployment		
16	Firewall Appliance should have a feature of holding multiple OS images to support resilience & easy rollbacks during the version upgrades		
17	Firewall Throughput should be equal to or more than 10 Gbps		
18	Firewall Throughput for multiprotocol / production performance should be atleast 2 Gbps		
19	The Firewall and IPS must support at least 75,000 new connections per second		
20	Appliance should have a capability to support for more than 500 VLAN & Should support 50 Virtual Context or more		
21	It should support the filtering of TCP/IP based applications with standard TCP/UDP ports or deployed with customs ports		
22	Firewall Modules should support the deployment in Routed as well as Transparent Mode		
23	The Firewall must provide NAT functionality, including dynamic and static NAT translations		

24	All internet based applications should be supported for filtering like Telnet, FTP, SMTP, http, DNS, ICMP, DHCP, ARP, RPC, SNMP		
25	Local access to the firewall modules should support authentication protocols – RADIUS & TACACS+		
26	The Firewall must provide filtering capability that includes parameters like source addresses, destination addresses, source and destination port numbers, protocol type		
27	The Firewall should reassemble the fragmented packets before examination		
28	It should support the VOIP Applications Security by supporting to filter SIP, H.323, MGCP and RTSP		
29	It should support the IPSec VPN for both Site-Site & Remote Access VPN		
30	IPSec ISAKMP methods should support Diffie-Hellman Group 1 & 2, MD5 & SHA , RSA & Manual Key Exchange Authentication, 3DES/AES-256 Encryption of the Key Exchange Material and algorithms like RSA-1024 / 1536		
31	Proposed solution should be member of VPNC / ICSA to ensure solution is highly interoperable in nature		
32	IPSec should have the functionality of PFS and NAT-T		
33	Firewall should support authentication proxy for Remote VPN, HTTP Applications Access, and various other applications		
34	Firewall should support PKI Authentication with PKCS#12 standards		
35	The Firewall should provide advanced NAT capabilities, supporting applications and services- like H.323 and SIP based applications		
36	Should support CLI & GUI based access to the firewall modules		
37	Proposed firewall should support DHCP Relay Agent functionality		
38	Should support secure access to corporate applications over the internet via Smart phones or PC's, Tablets and Laptops		
39	Solution should support integrated SSL VPN for access to various corporate applications like Web applications, File shares, Citrix services, Web Mail, Native applications etc.		
40	The Firewall VPN AES throughput should be equal to or more than 1 Gbps		
41	Should support the HTTP / HTTPS standards		
42	Should support HTTP / HTTPS and FTP filtering. Should support Java and Active-x filtering.		
43	A Dashboard facility providing total visibility of all related security events shall be included in the proposed system and customization based on severity defined by OICL		
44	Firewall should support site to site VPN Tunnels over IPV6 Addressing.		
45	Management Server should have the capability to centrally configure/manage all the firewall, VPN functions with logging & reporting capabilities.		

46	Management Server should monitor key health & performance for the firewalls & VPN services by providing network level visibility into device & traffic statistics. Eg: CPU & memory usage, interface status, dropped packets, tunnel status, connections/translations per sec, VPN & firewall throughput		
47	Management Server should provide firewall reports like top destinations, sources, services, Top bandwidth users for VPN, top duration VPN users, top throughput VPN users		
48	Firewall should support Identity Access for Granular user, group based visibility and policy enforcement.		
49	Integrated IPS functionality should be available as a module that can be activated and de-activated as and when required.		
50	IPS should have the functionality of Software Fail Open to enable firewall to be running always.		
51	The IPS should be constantly updated with new defences against emerging threats.		
52	IPS updates should have an option of Automatic downloads and scheduled updates so that it can be scheduled for specific days and time		
53	Intrusion Prevention should have an option to add exceptions for network and services.		
54	IPS should have advanced capabilities that detect and prevent attacks launched against the Web infrastructure		
55	Should support protections against Buffer Overflow, Heap overflow and other malicious executable code attacks that target Web servers and other applications.		
56	Should provide Application layer protections for Cross site scripting, SQL Injection, Command Injection, Directory traversal etc.		
57	IPS should be manageable from the Centralized console with detailed logging and event analysis		
58	Firewall & IPS should have integrated redundant power supply		
59	FW + IPS solution should support a minimum of 1,000,000 concurrent connection and provide a combined production throughput of atleast 2 Gbps		
60	Ability to identify attacks in IPv6 environments through the inspection of IPv4 traffic being tunnelled in IPv6		
61	IPS should be capable to inspect native IPv6 traffic		
62	Should support more than 3000 application layer and risk-based controls that can invoke tailored intrusion prevention system (IPS) threat detection policies to optimize security effectiveness.		
63	The solution must support creation of user-defined application protocol detectors.		
64	The solution support content awareness with comprehensive file detection policies and blocking of files by types, protocols and directions.		
65	- Protocols: HTTP, SMTP, IMAP, POP		
66	- Direction: Upload, Download, Both		
67	- File Types: Office Documents, Archive, Multimedia, Executable, PDF, Encoded, Graphics, and System Files.		

68	The detection engine should support capability of detecting and preventing a wide variety of threats (e.g., malware, network probes/reconnaissance, VoIP attacks, buffer overflows, P2P attacks, zero-day threats, etc.).		
69	The detection engine should support the capability of detecting variants of known threats, as well as new threats (i.e., so-called “unknown threats”).		
70	The management platform must be capable of aggregating IDS/IPS events and centralized, real-time monitoring and forensic analysis of detected events.		
71	The Quoted Security FW + IPS Device Series should be atleast EAL/NDPP/NSS Labs Certified		
72	Proposed Bidder must have a track record of continuous improvement in threat detection and must have successfully completed NSS Labs’ IPS Methodology testing with a minimum attacks /exploit blocking rate of 96% or more		
73	The proposed firewall OEM should be in the Leaders or Challengers quadrant of 2015 Gartner Magic Quadrant for Enterprise Network Firewalls		

13.1.18 Server Load Balancer

S.N.	Minimum Technical Specifications	Compliance (Yes/ No)	Reference in Enclosed Datasheet
	Hardware Specifications		
1	Should be Appliance based solution		
2	Solution should support minimum 20 Gbps L7 throughput		
3	Solution should support 25000 SSL TPS/CPS for 2048 bit key		
4	Should support SSL throughput of 15 Gbps		
5	Should have minimum 32GB RAM.		
6	Appliance Throughput upgrade should be done via software license (Should simultaneous Upgrade Compression / SSL throughput etc.)		
7	System should have at least 8x10G SFP+ Ports		
	Traffic Redirection		
8	System supports performing load balancing for Layers 4 through 7 of the Open Systems Interface (OSI) reference model with support to the IP, TCP and UDP protocols.		
9	System supports performing load balancing for Layers 4 through 7 based on source/destination IP		
10	System supports performing load balancing for Layers 4 through 7 based on application content		
11	System support load balancing based on relative weight		
12	System support load balancing based on cyclic (round-robin)		
13	System support load balancing based on least connections		
14	System supports virtual servers that can listen on UDP and TCP ports		
15	System has the ability to enable and disable individual servers behind a virtual address. Servers can be removed in both a graceful and hard shutdown fashion.		
16	The offered solution should provide the configuration wizards for LB etc.		
	Persistency		
17	System supports session persistency based on Layer 3.		
18	System is able to make persistency decisions based on cookies		
	Health Monitoring		
19	System supports the ability configure TCP and UDP monitors		
20	System supports HTTP health monitoring that mark nodes unavailable based on retrieval of a Web page for unique content		
21	System supports the ability to specify a minimum number of monitors to mark a Real Server as being available		
22	System supports multiple health checks per IP and per port		
23	System supports the ability to specify the number of retries for each monitor before marking a Real Server unavailable.		
24	System should support creating application specify custom monitor using scripts.		

	SSL Acceleration and Central		
25	System supports SSL offload - the ability to manage client side SSL traffic by terminating incoming SSL connections and sending the request to the server in clear text		
26	Should support end – end SSL if required		
27	System supports hardware based SSL acceleration		
28	System should support 1024, 2048 and 4096 bit key for SSL offloading		
	TCP Multiplexing		
29	System supports TCP Multiplexing		
30	System support HTTP connection pooling		
	HTTP Compression		
31	System supports HTTP compression		
32	Should support up to 6 Gbps of compression throughput		
33	Selective compression to avoid know compression problems in commonly used browsers		
	Mode of integration, IP Addressing (IPv4 and IPv6) and Routing features		
34	System supports one-arm , two-arm mode deployment		
35	System supports direct server return mode		
36	Should support IPv4 addressing		
37	Should support IPv6 addressing		
38	Should support IPv6 client and IPv4 servers		
39	Should support IPv4 client and IPv6 servers		
40	Should support routing protocols RIP/OSPF/BGP.		
	Global Server Load Balancing		
41	Global Server Load Balancing supported on the same appliance		
42	System supports performing load balancing across multiple geographical sites for transparent failover, complete disaster recovery among sites and optimal service delivery , Single application failure etc.		
43	System supports global response time optimization in real-time through advanced load and proximity measurements		
44	System supports providing failover capability between datacentres in active-active or active-backup modes		
45	System supports global redirection based on DNS		
	High Availability & Redundancy		
46	System supports active-active (AA) configuration		
47	System supports active-backup (AB) configuration		
48	System supports seamless failover between units in a pair		
	Management		
49	System supports Web Based Management for full device configuration (GUI)		
50	System supports modifying configuration via modular CLI		
51	System supports SSH and HTTPS access		
52	System enables to send logs to another server via Syslog		

53	System should support diagnostics which are readily available and easy to send to support (capture core dumps, configurations, logs, and so on).		
54	System should support Out of Box management if required.		
	Service ,Support & Training		
55	Bidder operates 24/7/365 global Technical Assistance Center (TAC)		

13.1.19 Application Delivery Controller

S.N.	Minimum Technical Specifications	Compliance (Yes/ No)	Reference in Enclosed Datasheet
	Hardware Specifications		
1	Should be Appliance based solution		
2	Solution should support minimum 20 Gbps L7 throughput		
3	Should support up to 25000 SSL Transactions per second (TPS) for 2048 bit key		
4	Should support SSL throughput of 15 Gbps		
5	Should have minimum 32GB RAM.		
6	Appliance Throughput upgrade should be done via software license (Should allow simultaneous Upgrade Compression / SSL throughput etc.)		
7	System should have at least 8x10G SFP+ Ports		
	Traffic Redirection		
8	System supports performing load balancing for Layers 4 through 7 of the Open Systems Interface (OSI) reference model with support to the IP, TCP and UDP protocols.		
9	System supports performing load balancing for Layers 4 through 7 based on source/destination IP		
10	System supports performing load balancing for Layers 4 through 7 based on application content		
11	System support load balancing based on relative weight		
12	System support load balancing based on cyclic (round-robin)		
13	System support load balancing based on least connections		
14	System supports virtual servers that can listen on UDP and TCP ports		
15	System has the ability to enable and disable individual servers behind a virtual address. Servers can be removed in both a graceful and hard shutdown fashion.		
16	The offered solution should provide the configuration wizards for LB etc.		
	Persistency		
17	System supports session persistency based on Layer 3.		
18	System is able to make persistency decisions based on cookies		

	Health Monitoring		
19	System should support the ability configure TCP and UDP monitors		
20	System should support HTTP health monitoring that mark nodes unavailable based on retrieval of a Web page for unique content		
21	System should support the ability to specify a minimum number of monitors to mark a Real Server as being available		
22	System should support multiple health checks per IP and per port		
23	System should support the ability to specify the number of retries for each monitor before marking a Real Server unavailable.		
24	System should support creating application specify custom monitor using scripts.		
	SSL Acceleration and Central		
25	System supports SSL offload - the ability to manage client side SSL traffic by terminating incoming SSL connections and sending the request to the server in clear text		
26	Should support end – end SSL if required		
27	System should support hardware based SSL acceleration		
28	System should support 1024, 2048 and 4096 bit key for SSL offloading		
	TCP Multiplexing		
29	System should support TCP Multiplexing		
30	System should support HTTP connection pooling		
	HTTP Compression and Caching		
31	System should support HTTP compression		
32	Should support up to 6 Gbps of compression throughput		
33	Selective compression to avoid known compression problems in commonly used browsers		
	Mode of integration, IP Addressing (IPv4 and IPv6) and Routing features		
34	System supports one-arm , two-arm mode deployment		
35	System supports direct server return mode		
36	Should support IPv4 addressing		
37	Should support IPv6 addressing		
38	Should support IPv6 client and IPv4 servers		
39	Should support IPv4 client and IPv6 servers		
40	Should support routing protocols RIP, OSPF and BGP.		
	Global Server Load Balancing		
41	Global Server Load Balancing supported on the same appliance		
42	System supports performing load balancing across multiple geographical sites for transparent failover, complete disaster recovery among sites and optimal service delivery , Single application failure etc.		

43	System supports global response time optimization in real-time through advanced load and proximity measurements		
44	System supports providing failover capability between datacentres in active-active or active-backup modes		
45	System supports global redirection based on DNS		
	High Availability & Redundancy		
46	System supports active-active (AA) configuration		
47	System supports active-backup (AB) configuration		
48	System supports seamless failover between units in a pair		
	Web Application Firewall		
49	The Web application firewall should address Open Web Application Security Project (OWASP) Top Ten security vulnerabilities such as SQL Injection, Cross-Site Scripting (XSS), Broken Authentication and Session Management.		
50	• The solution should prevent the following attacks (but not limited to): • Brute force • Access to predictable resource locations • Unauthorized navigation • Web server reconnaissance • HTTP request format and limitation violations (size, unknown method, etc.) • Use of revoked or expired client certificate • File upload violations		
51	Should meet all applicable PCI DSS requirements pertaining to system components in the cardholder data environment, should also monitor traffic carrying personal information.		
52	Should have the ability to inspect web application output and respond (allow, block, mask and/or alert) based on the active policy or rules, and log actions taken.)		
53	WAF should be able to block attacks based on IP source.		
54	Should inspect both web page content, such as Hypertext Mark-up Language (HTML), Dynamic HTML (DHTML), and Cascading Style Sheets (CSS), and the underlying protocols that deliver content, such as Hypertext Transport Protocol (HTTP) and Hypertext Transport Protocol over SSL (HTTPS). (In addition to SSL, HTTPS includes Hypertext Transport Protocol over TLS.)		
55	The WAF should have the ability to perform behavioural learning to examine traffic and highlight anomalies		
56	Transactions with content matching known attack signatures and heuristics based should be blocked		
57	The solution should support XML security (XML Denial of Service (xDoS))		
58	The solution should provide 1 Gbps of WAF throughput with all security features enabled.		
	Management		
59	System supports Web Based Management for full device configuration (GUI)		
60	System supports modifying configuration via modular CLI		

61	System supports SSH and HTTPS access		
62	System should enable to send logs to another server via Syslog		
63	System should support diagnostics which are readily available and easy to support (capture core dumps, configurations, logs, and so on).		
64	System should support Out of Box management if required.		
	Service ,Support & Training		
65	Vendor operates 24/7/365 global Technical Assistance Center (TAC)		

13.1.20 42U Rack

S.N.	Parameters	Minimum Technical Specifications	Compliance (Yes/ No)
1	Type	42 U Rack	
2	Rear door & front door perforations	Both front and rear doors must be at least 80% perforated (holes)	
3	Power Distribution Units	Should bear the 32A supply from IEC-309 Socket.	
4	Cable Management	19” Horizontal Cable Manager and Vertical cable manager	
5	Blanking Panels	15 blanking panel kit per rack.	
6	Depth	Should be provided according to requirement.	
7	Width	Standard, Bidder to specify	

13.1.21 IP Based KVM Switch

S.N.	Minimum Technical Specifications	Compliance (Yes/ No)
1	32 Ports IP Based KVM Switch	
2	Switch should have local console	
3	Switch should have remote console	
4	Minimum number of local concurrent user - 1	
5	Minimum number of remote concurrent users – 2	
6	Redundant Rack Power Cables	
7	Sufficient number of KVM, USB Conversion Cables.	

13.1.22 Mail Messaging Solution

S.N.	Minimum Technical Specifications	Compliance (Yes/No)
	MAIL SERVER	
1	The proposed mail solution software quoted should be commercially available software. The Bidder should indicate the latest version no, when it was released. Latest Version to be provided.	
2	The proposed messaging solution architecture should be centralized and in-premise solution	
3	The messaging solution should be actively supported by the OEM.	
4	The Proposed Messaging solution should not include any individual components running on Beta version	
5	The proposed Messaging Solution should support any one of the leading platforms like Windows, AIX, HP-UX, SUN SOLARIS, SUSE LINUX, RHEL.	
6	The proposed messaging solution should provide high availability and load Balancing capability.	
7	The Proposed messaging solution should provide access of mails via secured internet access and mobiles.	
8	DR should be configured for mail messaging solution.	
9	The messaging store should be database driven	
10	The proposed messaging solution should have built in server side filtering rule for messages.	
11	The proposed messaging solution should have option to define the maximum mail message size on a global/group/user level basis.	
12	The proposed messaging solution should support enhanced version of Mail Relay - TLS based relay	
13	The proposed messaging solution should support recalling/resending of messages sent and also should notify the user on the success or failure of the message recall. This facility should be available to users and administrators.	
14	On reaching quota limit, user should be able to delete mails but cannot send or forward mails on both Web and Native Clients.	
15	The proposed solution should provide Gateway servers for user access functions with capabilities like portal based Web Mail; push based mobile mail access, VPN less email access from internet.	
16	Email Server should have self-healing mechanism to automatically detect service depreciated or unavailable states and take automatic remedial steps like restarting the affected services, failing over user mailbox data to healthy servers etc. without admin intervention.	
17	Messaging store should provide for support for using SAN, DAS using SAS or SATA disks.	
	AUTHENTICATION	
18	The proposed messaging solution should relay mails only from authenticated users.	
19	The proposed messaging solution should relay the mails from the clients in the trusted network or to the domains that are configured as authorized relay destination.	
20	The proposed messaging solution should have Delivery Status Notification providing an e-mail sender ability to specify success, failure, delay or none of the message.	
21	The proposed messaging solution should support standard protocols like POP3/IMAP/HTTP and SMTP /MIME over normal and secure channels	
22	The proposed messaging solution should support multiple domains on a single system.	
	MAIL CLIENT	

23	Should provide an intuitive user interface	
24	Should support POP3, IMAP, HTTP, LDAP, SMTP based messaging servers	
25	Should support multiple email accounts in the same user interface for sending and receiving mails	
26	**Client should support rich editing features like:** - Tables - Support for embedded OLE objects - Horizontal line - Support for both Bullets and Number lists - Undo - Support a word Processing Application like MS Word as the default E-mail editor	
27	**Should support productivity enhancing features such as:** - Allow the user to raise a "flag" to alert the user that there is follow up action on the e-mail - Automatic background name resolution and type-ahead resolution prior to sending the mail -Multiple auto-signatures - Comprehensive message tracking details on a per message basis - Voting buttons with customizable selection criteria. Should support tracking of the responses received after the vote is over - Should notify a user visually or by sound, at user's choice, when a new message arrives. Should support message preview. - Should support Spell check and thesaurus integrated with the word-processing application installed on the clients computer	
28	**Should support rich attachments and interaction including:** - Viewing of file attachments from within message - Should support upto 100 attachments per email item. - Blocking of harmful, executable attachments (the extensions of which can be administratively controlled) - Allow attachment of text files, Word/Excel/PowerPoint documents, multimedia content, graphic files and non-Email documents	
29	Should support common messaging folders such as inbox, sent items, deleted items and productivity folders such as calendar, to-do list and personal addresses	
30	Should provide rich stand-alone/off-line access. The system should provide the same features available in either mode including access to the current corporate directory and all messages - Should store a copy of each item (including calendar, mail, to-do, personal addresses etc.) on the server and the client (while synchronizing with server in background) - Client should have the ability to rapidly and easily synchronize users' messages from the central message store to multiple stand-alone devices (i.e. laptop, desktop, handheld) securely over various network transports such as LAN, WAN, Dial-up, GPRS/GSM, Internet/VPN	
31	Should support personal user created folders which are portable from one system to another	
32	**Should provide auto-archival support:** - Users should have a capability to create local archival of the mails on their email client -Should support auto-archival on messaging folders and productivity folders - Should prompt the user before auto-archival starts. - Should provide the option of defining the time period to archive the mails - Should support the ability to add and delete from archives	

33	**Should provide easy methods for users to delegate or redirect inbox processing to others including support for:** - Delegating rights to other users on Inbox, Tasks, and Calendar Folders - Read, create, modify, no access permissions to the above mentioned folders. - Option of providing access for the delegate to items marked as private	
34	**Should support Rich Search capability:** - Find e-mail messages more easily by grouping messages by date, size, conversation, subject, importance, or other criteria - Save the results of commonly used searches instead of having to re-run common searches each time user need them providing an automated way to keep relevant e-mails together without moving them to other folders	
35	**Rich offline synchronization capability which includes:** - Support smart bandwidth awareness by switching message view to headers only or full message body depending on the connection speed - Client side caching where all messaging related tasks are performed from the local client machine to reduce number of requests to the server and reduce network bandwidth consumption between the client and server - Enable Incremental change synchronization so that client will start the synchronization process from where it left off last time saving time and resources - Enable Smart change synchronization to allow only changes and updates made to messages sent back to server instead of the entire message. - The user should be able to continue work in case of network unavailability without changing profile or closing the application.	
36	**Should support user controlled filtering and message manipulation rules including:** - Forwarding of, and response to, messages with a specified message template etc. - Client side and Server Side rules	
37	Should support exporting and importing of rules from one computer to another.	
38	Should support Email Delegation/Auto Vacation Message Reply while keeping a copy in user's inbox	
39	Messaging Client should provide Out-Of-Office notification of the recipients which composing the email so that sender doesn't waste time and can take informed decision on best method to communicate	
40	Messaging client should provide Recipient Mailbox full notification (as applicable) while composing the email, so that sender doesn't waste time in composing the mail	
41	Messaging client should support combining a sequence of tasks to a single click action to save time. For e.g. Composing a mail to pre-defined recipients with a specific subject line - is a set of activities which can be combined to achieve a single click action to achieve it. User should be able to associate a custom button to the task sequence on the Toolbar.	
42	The Solution should offer a feature where a user's could also restore a deleted mail by themselves within a set of specified days	
43	The messaging system should provide for connectors to common social networking sites.	
44	The messaging solution should be support for ignoring the messages tagged as SPAM/JUNK by the headers/subject or automatically SPAM/JUNK Message should go to SPAM/JUNK Folder.	
	WEB INTERFACE	

45	All Web mail functionality should be accessible through all supported web browsers including Internet Explorer, Mozilla Firefox in the proposed messaging solution	
46	The Web mail client should provide access to email over low bandwidth connection using Basic / Light Mail client functionality.	
47	The proposed messaging solution should support timeout to automatically sign off an user if the system detects a prolonged period of inactivity.	
48	The proposed messaging solution should have rich, interactive, web-based interface for end user functions (accessible via HTTP or HTTPS)	
49	The proposed messaging solution should support automatic and manual refresh of the user interface to automatically display newer messages and other updates	
50	The proposed messaging solution should provide administrators the ability to define web mail session idle time at the global level	
51	The proposed messaging solution web interface should have Secure logout from Web mail client to prevent unauthorized access to mail pages after sign out.	
52	The proposed messaging solution should support customization of look and feel with different Color themes of the web mail client	
53	The proposed messaging solution should allow users to search from within the web client.	
54	The proposed messaging solution should support auto address completion including stored email addresses as they are being typed, including a dynamically updated selection dialog when multiple addresses match.	
55	The proposed messaging solution should provide the ability to assign tags/categories to To-Do, Contacts, and Calendar entries. Ability to assign tags to mail messages	
56	The proposed messaging solution should have a built-in rich text editor for composing messages with support for color, fonts, attributes, font size, hyperlinks, etc.	
57	The proposed messaging solution should provide users ability to choose from recipients stored in personal Address Books, shared Address Books, or the Global Address List.	
58	The user should be able to append a text signature.	
59	The proposed messaging solution Web Interface should have user definable personal folders to organize mail.	
60	The proposed messaging solution web interface should support email addressing and look up from Global address book for wide list of contacts, group mailing etc.	
61	The proposed messaging solution web interface should support read receipt request - while composing a message, user can mark the message to request for a read receipt notification from the recipient and delivery status notification.	
62	The proposed messaging solution should support Message Priority feature - to set priority of messages while composing them	
63	The proposed messaging solution should support filtering of incoming mails based on user definable filtering rules.	
64	Webmail interface should have features for notification of new mails	
65	Webmail interface should have an integrated calendar providing the following features: shared calendar, to-do lists, event scheduler and reminders	
66	The user should be able to change the password through web interface	
67	User should be able to mark mails as read or unread and maintain flags for follow ups	

68	The Webmail interface should provide feature to search messages based on: From, To, Cc, Subject and body but not limited to these, search in the folders and also advance search capabilities.	
69	User should be able to flag important email items for the purpose of follow-up, indicated by a flag in the inbox.	
70	Web Mail Client should let users track their message to ensure success of delivery to the recipient	
71	Web Mail Client should let users remotely wipe data from their Mobile devices without IT intervention, in case of device lost situations etc.	
72	The mail messaging solution Should support basic authentication, session authentication, secure logoff, Secure Sockets Layer encryption	
73	Users should be able to access web mail using a common URL published for the email site.	
74	Users should be capable of viewing the total size and available space of their mail boxes	
75	Web Mail Client should provide capability of Offline Access, so that users can work on email, even if network connection is not there. This feature should be supported on all major browsers including IE, Chrome & Firefox.	
76	The Web Mail client should provide ability to access delegated mailbox from the logged on web mail client.	
77	The Web Mail client should provide ability to add sender to Blocked Sender list or Safe sender list.	
78	The Web mail client should provide an alert for any external recipients whenever forwarding or replying to email, so user can take self-precautions of not sending any sensitive content.	
	CALENDARING	
79	**Should natively support server-side and client-side calendaring and scheduling, including:** - Checking the online availability of intended attendees for a meeting - Sending of request for meetings - Accept or reject meeting requests - Provide conflict management for meetings - Reply to requests for meeting with a newly proposed time and date - Should automatically recommend ideal meeting times when all/most people are available.	
80	Should Support Meeting Requests, Forward Meeting Requests and Generate Alerts.	
81	Should support accessing a group calendar to view simultaneously the free time schedules of 2 or more users or resources	
82	It should be able to suggest best timing for meetings based to participants availability by using Scheduling Assistant, Attendance Confirmation.	
83	Should support tracking of responses from the meeting invitees with information on the number of accepted and rejected responses.	
84	Should support marking appointments as private, so it will not appear when others view ones calendar.	
85	Should support vCalendar standard	
86	User should be able to view selected days or series of days apart from default views like Daily, Weekly, Monthly, and Calendar List, to do List.	
87	An incoming meeting request should be stored in the calendar as “Tentative” automatically. Once the user accepts the meeting invite, an automatic reminder with audio/visual alarm should be added into the calendar	
88	Should support access to multiple calendars side by side to make scheduling meetings fast and more convenient.	
89	User should be able to customize a work week by Days and hours.	

90	Should support Schedulable Out of Office. Out of Office messages should be scheduled to begin and end at given dates/times. It should support for separate out-of-office messages to be set for internal and external recipients, Should support Blocking Out of Office messages from distribution lists-Out of Office messages should not be sent to the entire membership of a distribution list that is listed in the To or Cc boxes.	
91	The Messaging solution should support the ability to create shared team Calendar and tasks	
92	The messaging solution should provide resource scheduling like conference rooms etc. These shared resources should also provide info like location, Room Capacity, features like Projector, Whiteboard etc.	
93	The messaging solution should have wide administrative capabilities to control over calendaring.	
	TASKS	
94	Should support server-side and client-side Tasks (or To Do List) and should support assigning tasks to other users in the messaging system	
95	Create tasks automatically linked to a contact (address book entry) and view tasks grouped by contact	
96	Should provide the ability to assign due dates to “To Do” items.	
97	Should provide the ability of accepting, rejecting or updating the “To Do” item that has been received from other associates.	
98	Should allow a “To Do” owner to check the status of assignees.	
99	Should allow a “To Do” assignee to accept, delegate, or request modifications to a “To Do”	
100	Should provide the ability to receive notifications of upcoming due dates.	
101	Should support delegating the authority to others to manage your “To Do” list.	
	ADDRESS BOOK	
102	The Mail Messaging Solution Ability to index Corporate Address book and personal address book alphabetically. All address books must available to the users through rich client, web client and supported mobile devices.	
103	Should provide Offline Address Book Support as follows: - The Directory Services should provide an interface for messaging clients to download the address book to their local machine and work offline - The client should also offer the functionality of partial or full download of the address book locally - The synchronization should download only the new information and not re-download the old information already present on the client end	
104	The user should be able to add/delete/modify the contacts in address book via email client, web client and mobile client	
105	Should support personal directory apart from the offline address book	
106	When user copies a contact from Corporate Address book to their local contact store in email client, then any critical changes (like address, phone number etc.) to the contact at Corporate address book level, it should automatically get updated to user's copy of the contact in their Personal Address Book.	
107	The messaging solution should provide user self-service capability for Email Group Membership Management	
108	Users can add addresses from other organizations or individuals to their private address book	
109	Messaging solution should support server-side and client-side contact management including integration of contacts with word processing applications	
	MOBILE ACCESS	

110	The proposed messaging solution should support and be configured for push based emails on popular mobile platforms: Windows, Android and IOS	
111	The mobile platform should provide native support for connectivity to Messaging server.	
112	The Mobile client should support SSL based authentication	
113	Should support synchronization of calendar items, contact items, and mail items between smartphone devices and the messaging server over Mobile data network over the Internet	
114	The users should be able to synchronize tasks between their mobile devices and the messaging solution	
115	The users should be able to search the corporate contacts directory from their mobile devices	
116	The users should have the functionality to search through their mailbox from their mobile devices.	
117	The user should be able to configure Out of office messages from their mobile devices	
118	The proposed messaging solution should be configured for security policy (Password policies) enforcement and remote erase capability for smartphones to protect data on supported mobile devices	
119	The solution should support encryption on device and memory card to prevent unauthorized access of data on supported mobile devices	
120	The proposed messaging solution should allow end-users to remotely wipe their mobile devices via the messaging client web interface, rather than over-burdening the IT helpdesk with support requests for the same.	
121	Mobile Security policies should support capabilities to disable Camera and Browser on supported devices.	
	SYSTEM ADIMINSTRATION & MAINTENANCE FEATURES	
122	Should be capable of administration through a single window interface to provide server level control and configuration of the messaging system for all servers including: - Create / rename / delete mail accounts - Reset / set user passwords for both Directory & Messaging platform - List all users in the messaging system - Search for a user and modification of user object attributes - Enable / disable user accounts - Change delegated administration passwords - Add alias e-mail address for a user	
123	The proposed messaging solution should avoid mail loops when auto responding – i.e. should not send auto responder to every mail received from a particular sender with in the defined vacation duration.	
124	The messaging solution should be support for ignoring the messages tagged as SPAM/JUNK by the headers/subject or automatically SPAM/JUNK Message should go to SPAM/JUNK Folder.	
125	The proposed Messaging Solution should allow end Users to create and delete specific distribution groups, as well as manage memberships and ownership as a self-help service.	
126	The User should be able to change their password	
127	The proposed messaging solution should have the ability to enforce following features of a password	
128	Password length should be minimum 8 characters	
129	Password should support Alpha numeric & Special characters like a-z, A-Z,0-9,!@#$%^&*	
130	Change of Password at regular interval feature should be provided	

131	The proposed messaging solution should allow for password lockout for Web Users when they input the wrong password	
132	The proposed messaging solution should maintain the password history.	
133	The proposed messaging solution should support the ability for administrators to age e-mail for deletion.	
134	The proposed messaging solution should prevent any script written by a user (internal / external) from executing on the client machine unless the same has been certified by the system administrator	
135	The proposed messaging solution should provide administrators ability to perform queue handling tasks such as delete, redirect, flushing.	
136	System should be able to generate exception reports on mailbox access by non-owners to ensure admin/delegation permissions in line with the security standards.	
137	The proposed Messaging solution should allow to track message delivery	
	MESSAGE ROUTING	
138	Should support SMTP as the default messaging protocol for mail transfer between messaging servers.	
139	Should support fault-tolerant SMTP routing between servers.	
140	Should be a messaging system that works with the existing network topologies and has the ability to customize the mail delivery routes between messaging servers in various physical locations over the WAN setup.	
141	Should support least cost, load balanced and dynamic mail routing	
142	The messaging Server should support redundancy of incoming SMTP email queue by replicating it to another server in the cluster or site. In case of primary server failure, the redundant queue can be used to resubmit email, to ensure no data is lost.	
	MAIL SECURITY	
143	The proposed messaging solution should provide SSL/TLS and MIME support for encrypted communication.	
144	The proposed messaging solution should be able to validate sender domain in DNS (Sender Policy Framework)	
145	The proposed messaging solution should be protected from Denial of Service Attacks	
146	The Proposed Messaging Solution should automatically warn users if recipients outside the organization are present in the email they are responding to, so they can take informed decision about any information being sent to external parties.	
147	The messaging solution should be able to take specific corrective action like blocking or redirecting email based on different criteria such as email from specific users, with specific keywords, with specific attachments/file extensions	
148	The messaging system should encrypt message exchange between the messaging client and the messaging server, including support for : Native S/MIME Encryption of the client-server and server-server communication	
149	The system should provide ability to block communications between two different users/groups in the same organization and should be able to send notification.	
150	The Proposed messaging solution should have capability to automatically insert disclaimers for emails going outside the organization.	
	Email Archival and Compliance	
151	The proposed solution should provide compliance archival for all mail boxes on the server side to be used by Compliance officer, Auditors and Administrator for Audit and Backup/restore purpose. Email Data retention is for 6 years	

152	The system should allow server side rules for retention of internal, external mails to be journal/saved to a separate database	
153	Based on administrator defined rules, a copy of the mail should go to Journaling database & retained there for desired time for audit purposes	
154	Only authorized administrators will have access to search the mails rom the compliance database	
155	Administrator should be able to search individual or all mailboxes based on keywords, date, from, To/cc/bcc etc.	
156	Solution should support per user Mailbox archive at the server level, for storing / retaining email data Ability to automatically transfer emails from Primary mailbox to archive based on retention policies. Ability to delete email post the retention cycle should be available on the Server Side Archive	
157	The solution should support access to Archive both from email client and Web Based email access.	
158	Solution should be able to enforce email retention settings on users so emails can be retained/archived/deleted as per compliance policies.	
159	The system should allow server side rules for retention of all or specific items in the Email default folders like Inbox.	
160	Solution should support email data tamper-proofing capabilities for immediate preservation of email which is changed or deleted by user (Like mail, appointments, tasks, etc.) from both their primary mailbox and Archive. Email Tamper-proofing can be set on individual mailboxes, across the enterprise; it can be time-bound Hold or specific email data that fits particular criteria. Archived email data should be held outside the email server User should have seamless access to their respective archived e-mails.	
161	Solution should be able to enforce email retention settings on users so emails can be retained/archived/deleted as per compliance policies.	
162	The proposed solution should provide e discovery capabilities to set Search filters for quick searching data within multiple Mailboxes, Personal Archives & data held via tamper-proofing through single interface.	
163	Archived E-mails should be kept in a de-duplicated format for space efficiency on archive repository.	
	Eligibility criteria for proposed E-mail solution (Relevant documents to be submitted)	
164	The Proposed Messaging solution should be Enterprise Grade. It should have a proven deployment track record and should be successfully running at minimum three Indian BFSI organizations with atleast 5000 mailboxes in each organization.	
165	The Proposed Product “Messaging Suite” should have been implemented by at least five organizations, with minimum of 10000 mailboxes in each organization.	

13.1.23 Proxy Server Solution

S.N.	Minimum Technical Specifications	Compliance (Yes/No)
A	**General**	
1	The solution should be appliance based with Web Proxy, Caching, SSL Decryption, Dynamic URL Filtering, Reputation based Filtering, Advanced Application Control, Real Time Security Scanning and Classification, in a single appliance.	
2	Solution should be deployed in High Availability (HA) Mode at DC and Non-HA Mode at DR Site.	
B	**Proxy & Caching Deployment Options**	
1	The solution should support explicit forward proxy mode deployment	
2	The forward proxy mode deployment should support single IP proxy configuration and dual IP proxy configuration where one IP will be of local LAN and other IP will be of DMZ	
3	The solution should also support transparent mode deployment using to avoid proxy bypass using proxy avoidance tool	
4	The solution should allow Virtual IP failover so that if a node in the cluster fails, other nodes can assume the failed node's responsibilities.	
5	The solution must be capable of high availability deployment configurations to provide continuity of protection in case of a partial or total system, hardware or facility failure.	
6	The solution should support configuration to use Split DNS. It should be able to refer to different DNS for Different Domains (e.g. root dns for all external domains and internal DNS for organization domain)	
7	The solution should have the facility to do IP spoofing. When enabled, requests originating from a client should retain the client's source address and appear to originate from the client instead of the appliance.	
8	The solution should do prioritization of specific website or application traffic by source, destination and/or content - prioritized by user, group, business unit or time of day.	
C	**Threat Prevention**	
1	The solution must detect and block outbound Botnet and Trojan malware communications from infected systems. System must log and provide detailed information on the originating system sufficient to enable identification of infected units for mitigation.	
2	The solution shall be capable of dynamically blocking a legitimate website which has become infected and unblock the temporary site restriction when the threat has been removed.	
3	The solution shall protect against known binary executable, script based exploits, Key Loggers and obfuscated code or scripts entering the network.	
4	The solution should be able to stop proxy avoidance software/websites like TOR, Ultrasurf, GhostSurf, JAP, RealTunnel etc.	
D	**Proxy Requirement**	
1	The proposed solution should be a Fast Web Proxy and should support HTTP, FTP and HTTPS proxy. The solution should also support HTTPS decryption and scanning.	
2	The solution should support to tunnel certain ports via HTTP e.g. Tunnelling FTP via HTTP.	
3	Solution should support the maximum number of protocols.	

4	The solution should allow administrator to define access to internet based on IP addresses, ranges of IP addresses, subnet, users from Active Directory/LDAP, CIDR basis.	
5	The solution should support Multiple Authentication Servers / Auth. Failover using Multi Scheme Auth (NTLM and LDAP).	
6	Should support policy based HTTPS decryption based on URL Categories and/or Web Reputation scores in order to enforce acceptable use and security policies on decrypted data.	
E	**Caching Requirements**	
1	Should Have Inbuilt Caching Mechanism.	
F	**Security**	
1	Solution should have an inbuilt Anti Malware, antivirus engine that can scan HTTP, HTTPS and FTP traffic for web based threats, that can range from adware, browser hijackers, phishing and pharming attacks to more malicious threats such as rootkits, Trojans, worms.	
2	Enhance category-based filtering with real-time scoring based on reputation of website content sources that uses a multi-point reputational analysis.	
G	**Web Content, Social Web, Video Controls, URL Filtering**	
1	The solution should be able to provide controls to restrict Posts, Upload Photos, Videos etc to the social networking websites.	
2	The solution should be able to provide categories for Entertainment, Educational and Viral Videos that exist on sites like YouTube.	
3	The Web Reputation Filters should have the capability to analyse different types of web traffic.	
H	**Traffic Inspection**	
1	The solution should be able to do URL filtering for HTTP and SSL traffic by redirecting only the get request to the server deployed in the corporate network for policy enforcement.	
I	**Administration and Management**	
1	The appliance should be manageable via HTTP, HTTPS, Command Line using SSH, serial console access	
2	The appliance should be able to export policies to a restorable file.	
3	The appliance should have a management console that can run on remote machine through a web browser	
4	It should be possible to permit remote management of the appliance from specified IP address only	
J	**Logging and Reporting**	
1	The retention period should be customizable. Options should be provided to transfer the logs to an FTP server using FTP or SCP or via tape drive using database backup.	
2	The solution should provide detailed reporting activity.	
3	The solution should provide reports on Bandwidth Consumed.	
4	The solution should maintain detailed proxy access logs that can be searched via filters.	
5	The Proposed Solution should Integrate seamlessly with existing Active Directory Solution.	

13.1.24 DR Management Software

S.N.	Minimum Technical Specifications	Compliance (Yes/No)
1	The proposed solution should be in the form of software which is rated/ mentioned in independent analyst reports from either Gartner or IDC.	
2	The proposed solution must offer a workflow based management & monitoring capability for the real time monitoring of a DR solution parameters like RPO (at DB level), RTO, replication status and should provide alerts on any deviations.	
3	The proposed solution should provide a single dashboard to track DR Readiness status of all the applications under DR.	
4	The proposed solution should be capable of reporting important health parameters like disk space, password changes, file addition/deletion etc. to ensure DR readiness and facilitate policy based actions for events with ability to cancel out polar events.	
5	The proposed solution should have inbuilt ready to use library of recovery automation action for heterogeneous databases and replication environment. This must significantly reduce custom development of scripts and speedy deployment of DR solutions.	
6	The DR Management solution should have a managed lifecycle for all workflows from draft to final published version with version control and time stamp to ensure proper testing and troubleshooting of drill/recovery procedure.	
7	The proposed solution should be capable of executing DR drill and recovery workflows in simulation mode, without any changes to DR to ensure conditions are met for a successful execution.	
8	The proposed solution should be capable of generating reports and email/SMS alerts on RPO deviation, RTO deviation and DR Drills from a centralized location.	
9	The proposed solution should be able to manage hosts by either deploying agents or without deploying any agent and should seamlessly integrate with existing environment without the need to replace/change configuration including existing clusters.	
10	The proposed solution must support all major platforms including Linux, Windows, Solaris, HPUX, and AIX with native high availability options. It must support both physical and virtual platforms.	
11	The proposed solution should have file level replication for associated application servers and DB log replication which is supported on the commonly used OS platforms and has inbuilt bandwidth compression.	
12	The proposed solution should have a file system analytics tool to give total file/directory count, typical scan time, number of open files, time of last replication for a file, file size and time stamp.	
13	The DR Monitoring and Management software must be running successfully in at least 10 organizations.	
14	The DR Monitoring and Management software must be available in Indian market for more than 6 years and running in at least 3 organisations in financial sector.	
15	The main management server of the proposed should have a mechanism to have a local HA and remote, real time replica to eliminate any single point of failure and should not have any impact on the production in case the main management server fails.	

16	The DR Management solution should be tested and certified by a third party Organization to ensure that there are no security vulnerabilities which can be exploited.	
17	The DR management solution should have inbuilt debugging and log capture with facility to view the logs from the web based GUI itself.	
18	The DR Management solution should have a validation tool to verify DC-DR equivalence for OS, databases and applications with both out-of-box and custom templates.	

13.1.25 Desktop

S.N.	Description	Mandatory Technical Requirements	Compliance (Yes / No)
1	Processor	Intel core i7 4th Generation (3.2 GHz or Higher, 8 M Cache or higher)	
2	Chipset	Latest compatible chipset supporting above processor.	
3	Motherboard	OEM Motherboard.	
4	Memory	8 GB RAM	
5	Internal Hard Disk	1 TB or more SATA	
6	Optical Drive	DVD Writer	
7	Graphics	Integrated Intel HD Graphics supporting VGA and DVI (optional) based monitors.	
8	Ethernet Controller	Embedded auto sensing 10/100/1000 Mbps with remote boot features (PXE Boot)	
9	Cables & Connectors	Power cords for CPU and Monitor Connecting cord for monitor and display adapter	
10	Slots & Ports	6 External USB Ports (2 front , 4 Rear) 1 Serial, 1 VGA video 1 RJ-45 1 line in,1 line out 1 PCI e x 16	
11	Monitor	21" or higher LED wide screen color monitor (same brand as Desktop) with speakers , TCO 05 Complied, 32 bit colors or higher	
12	Keyboard	USB 104 keys Bilingual (English / Hindi) , color as base PC	
13	Mouse	USB optical scroll OEM mouse and mouse pads of superior quality.	
14	Operating system	Preloaded latest version of, Windows 10 or latest Professional with latest service pack (license included). Each PC should be supplied with: 1.OS, Recovery mechanism to be provided for OS Restoration. 2. Product documentation CD / manuals.	
15	Security Feature	Security loop for external lock , boot sequence control , power - ON & BIOS configuration password	
16	Certification-	Windows 10 or above Certified, ISO 9001 & 14001 Certified for manufacturing of PC's from OEM.	

13.2 Annexure 2 : Evaluation Methodology

The competitive bids shall be evaluated in three phases:

Stage 1 – Eligibility criteria

Stage 2 – Technical Bid

Stage 3 – Commercial Bid

Stage 1 – Eligibility Criteria Evaluation

Eligibility criterion for the Bidders to qualify this stage is clearly mentioned in Section 1.6 - Eligibility Criteria of this document. The Bidders who meet ALL these criteria would only qualify for the second stage of evaluation. The Bidder would also need to provide supporting documents for eligibility proof. All the credentials of the Bidder necessarily need to be relevant to the Indian market.

The decision of OICL shall be final and binding on all the Bidders to this document. OICL may accept or reject an offer without assigning any reason whatsoever.

Stage 2 - Technical Bid Evaluation

Total Marks 500. Minimum Overall Qualifying marks to become eligible for qualifying for Commercial Evaluation are 70% i.e. 350 out of 500.

Category	Criteria	Max Marks
A.	Bidders Project Experience	150
B.	Response to RFP & Design, Implementation & Project Management	200
C.	Bidders Technical Presentation	150
	Total	**500 Marks**

It is mandatory for the Bidder to comply with all the line items given in the technical specifications (Annexure 1). In case if the Bidder does not comply with any of the line items given in technical specifications (Annexure 1), it will not qualify to Stage 3 of evaluation process even if they score the cut-off marks in Stage 2.

OICL at its discretion may reject the proposal of the Bidder, without giving any reason whatsoever, if in case the submission/responses received from the Bidder were found to be unsatisfactory.

Page **132** of **155**

A. Bidders Project Experience

S.N.	Bidder's Profile & Project Experience	Marks Allocation	Max Marks	Support Documentary Proof
1	The Bidder should have executed System Integration Projects involving delivery, installation and maintenance of IT Solutions like Servers, Storage, Backup, Network Switch, Firewall, Application Delivery Controller, Server Load Balancer, DR Management Tool, Mail Messaging in Government/ PSU/ BFSI sector in India in the last 5 years. (Value of each project should be more than INR 10 Crores and should consist of atleast 3 IT Infrastructure components mentioned above.)	>= 4 Projects : 40 3 Project : 30 2 Project : 20	40	Copy of original PO / Contract highlighting the following: a) Date of PO / Contract b) Name of Parties c) Scope of Work.
2	The Bidder should have executed project for delivery, installation and maintenance of Enterprise Class Storage of worth atleast 2 crore in Government/ PSU/ BFSI sector in India for last 5 years.	>= 2 Projects : 20 1 Project : 10	20	
3	The Bidder should have executed project for delivery, installation and maintenance of Core Networking / Firewall / ADC / SLB in Government/ PSU/ BFSI sector in India for last 5 years.	>= 2 Projects : 20 1 Project : 10	20	
4	The Bidder should have executed project for implementing Mail Messaging Solution in Government/ PSU/ BFSI sector in India for last 5 years	>= 2 Projects : 15 1 Project : 10	15	
		>=5000 Users in one PO: 15 2000 Users in one PO: 10	15	
5	The Bidder should have implemented DR Management Tool in Government/ PSU/ BFSI sector in India for last 5 years	>= 2 Projects : 20 1 Project : 10	20	
6	The Bidder should have provided 24x7 onsite services to client / monitoring services from their NOC to manage customers IT infrastructure in Government/ PSU/ BFSI sector in India for last 5 years	>= 2 Projects : 20 1 Project : 10	20	
			150 Marks	

B. Response to RFP & Design, Implementation & Project Management

S.N.	Response to RFP & Design, Implementation & Project Management	Marks
1	Understanding OICL's scope of work and requirements	30
2	Detailed Proposed Solution with Solution Architecture	50
3	Proposed Products – Key Features and Functionalities	20
4	Detailed Migration Methodology	50
5	Proposed Facility Management Service • 24x7 onsite support experience • Advanced Monitoring and Reporting Service	30
6	Project Plan / approach/ implementation methodology	20
	Total	**200 Marks**

C. Bidder's Technical Presentation:

The Bidders, who have qualified stage 1, will be required to provide a technical presentation to OICL.

The Bidders will be required to make presentations highlighting the various aspects of the proposed solutions. This process will also enable OICL to clarify issues that may be identified from the Bidders' responses to the RFP. The Evaluation Committee decided by OICL will be scoring the presentation made by the Bidders based on a structured questionnaire broadly across the following indicative sections. The Bidder technical presentation will be scored out a total of 150 marks.

S.N.	Evaluation of the Bidder Presentation	Marks
1	Project Execution Methodology and Risk Mitigation Plan	10
2	Detailed Proposed Solution with Solution Architecture	30
3	Detailed Migration Methodology	40
4	Proposed Facility Management Service • 24x7 onsite support experience • Advanced Monitoring and Reporting Service	40
5	Adherence to Timelines / Project Plan	10
6	Post Implementation Support : Approach and Resource Commitment	20
	Total Bidder Technical Presentation	**150 Marks**

Stage 3 – Commercial Bid Evaluation

The commercial bids for the technically qualified Bidders will be opened and reviewed to determine whether the commercial bids are substantially responsive. Bids that are not substantially responsive are liable to be disqualified at OICL'S discretion. The total cost of ownership for the purpose of evaluation shall be calculated over the contract period of 6 years. At the end of 6 years, the contract may be re-negotiated as mutually agreed by both parties.

OICL will award the contract to the successful Bidder whose bid has been determined to be substantially responsive and has been determined as the lowest commercial bid (L1), provided further that the Bidder is determined to be qualified to perform the contract satisfactorily.

13.3 Annexure 3 : Authorization letter to attend tender opening

To

The Deputy General Manager
Information Technology Department
The Oriental Insurance Company Limited
2nd Floor, Head Office, “Oriental House”
A-25/27, Asaf Ali Road
New Delhi - 110 002

Sir,

Reference: Tender No. OICL/HO/ITD/TECH-REFRESH/2015/01 Dated 28th August 2015

Mr. /Ms..... has been authorized to be present at the time of opening of above tender due on ..... at ..... on my/our behalf.

Yours faithfully

Signature of Bidder

Copy to: Mr/Ms.....……for information and for production before the Tender Opening Committee at the time of opening of bids.

13.4 Annexure 4 : Details of Similar Projects Undertaken in last 5 Years

S.N.	Criteria	Name of Client	Contact Details of Senior Official of Client	Date of Award of Project	Current Status of Project
1	The Bidder should have executed project for delivery, installation and maintenance of Servers, Storage, Backup, Network, Security, DR Management, Mail Messaging etc. (any three technologies) in Government/ PSU/ BFSI sector in India for last 5 years.	1. 2.	1. 2.	1. 2.	1. 2.
2	The Bidder should have executed project for delivery, installation and maintenance of Enterprise Class Storage of worth atleast 2 crore in Government/ PSU/ BFSI sector in India for last 5 years.	1. 2.	1. 2.	1. 2.	1. 2.
3	The Bidder should have executed project for delivery, installation and maintenance of Core Networking and Firewall in Government/ PSU/ BFSI sector in India for last 5 years.	1. 2.	1. 2.	1. 2.	1. 2.
4	The Bidder should have executed project for implementing Mail Messaging Solution in Government/ PSU/ BFSI sector in India for last 5 years	1. 2.	1. 2.	1. 2.	1. 2.
5	The Bidder should have implemented DR Management Solution in Government/ PSU/ BFSI sector in India for last 5 years	1. 2.	1. 2.	1. 2.	1. 2.
6	The Bidder should have provided 24x7 onsite services to client / monitoring services from their NOC to manage customers IT infrastructure in Government/ PSU/ BFSI sector in India for last 5 years	1. 2.	1. 2.	1. 2.	1. 2.

13.5 Annexure 5 : Application form for Eligibility Bid

APPLICATION FORM FOR ELIGIBILITY BID (Page 1)

To,

The Deputy General Manager,
Information Technology Department,
The Oriental Insurance Company Limited,
2nd Floor, Head Office, "Oriental House",
A-25/27, Asaf Ali Road,
New Delhi - 110 002

Reference: Tender No. OICL/HO/ITD/TECH-REFRESH/2015/01 Dated 28th August 2015

Company Details

1.	Registered Name & Address of The Bidder	
2.	Location of Corporate Head Quarters	
3.	Date & Country of Incorporation	
4.	Sales Tax/ VAT registration number and date of registration	
5.	Service Tax registration No. and date of registration	
6.	Address for Communication	
7.	Contact Person-1 (Name, Designation, Phone, Email ID)	
8.	Contact Person-2(Name, Designation, Phone, Email ID)	

Turnover and Net worth:

Financial / Accounting Year	Turnover (Rs Crores)	Net worth

Details of EMD (BG)

Description	₹ 4,00,00,000/- BG towards EMD

APPLICATION FORM FOR ELIGIBILITY BID (Page 2)

Service Center – Delhi / NCR

Contact Person	
Address	
Contact Number	
Email ID	

Service Center – Mumbai

Contact Person	
Address	
Contact Number	
Email ID	

Service Center – Bengaluru

Contact Person	
Address	
Contact Number	
Email ID	

Signature: _____

Name: _____

Designation: _____

Date: _____

(Company Seal)

13.6 Annexure 6 : Contract Form

THIS AGREEMENT made on this _____ day of _____ between The Oriental Insurance Company Limited (hereinafter "the Purchaser") of one part and "<Name of Bidder>" (hereinafter "the Bidder") of the other part:

WHEREAS the Purchaser is desirous that certain software and services should be provided by the Bidder viz., _____ and has accepted a bid by the Bidder for the supply of those software and services in the sum of _____ (Contract Price in Words and Figures) (hereinafter "the Contract Price").

NOW THIS AGREEMENT WITNESSETH AS FOLLOWS:

In this Agreement words and expressions shall have the same meaning as are respectively assigned to them in the Conditions of Contract referred to.

The following documents shall be deemed to form and be read and construed as part of this Agreement viz.

The Schedule of Requirements and the Requirement Specifications

The Service Level Agreement

The General Conditions of Contract

The Purchaser's Notification of Award

In consideration of the payments to be made by the Purchaser to the Bidder as hereinafter mentioned, the Bidder hereby covenants with the purchaser to provide the hardware, associated software, and services and to remedy defects therein the conformity in all respects with the provisions of the contract.

The purchaser hereby covenants to pay the Bidder in consideration of the provision of the hardware, associated software, and services and the remedying of defects therein, the contract price or such other sum as may become payable under the provisions of the Contract at the times and in the manner prescribed by the Contract.

Brief particulars of the goods and services, which shall be supplied/ provided by the Bidder, are as under:

Item No.	Description of the Item	Quantity	Price per Unit*	Total Price	Payment Terms

* Break-up would be as per commercial bid format

Total Value: _____

Delivery Schedule: _____

IN WITNESS where of the parties hereto have caused this Agreement to be executed in accordance with their respective laws the day and the year first above written.

Signed, Sealed and Delivered for "The Oriental Insurance Co. Ltd." by it's constituted Attorney		**Signed, Sealed and Delivered for M/s _____ by its constituted Attorney**	
Signature	_____	Signature	_____
Name	_____	Name	_____
Designation	_____	Designation	_____
Address	_____	Address	_____
Company	_____	Company	_____
Date	_____	Date	_____
Company Seal		**Company Seal**	
Witness I		**Witness II**	
Signature	_____	Signature	_____
Name	_____	Name	_____
Designation	_____	Designation	_____
Address	_____	Address	_____
Company	_____	Company	_____
Date	_____	Date	_____

13.7 Annexure 7 : List of Buy-Back Equipment

13.7.1. Buy-Back Items: Bengaluru

S.N.	Model	Make	Qty	Purpose	Year of Purchase
Servers					
1	T5120	Sun	1	Mail MTA (DR)	2009
2	T5120	Sun	1	On-site T&D	2009
3	T2000	Sun	1	Not in Use	2007
4	T2000	Sun	1	Proxy BNG	2007
5	V480	Sun	1	Oracle Enterprise server	2005
6	M4000	Sun	1	Backup Server	2009
7	SB6000 Blade Chassis	Sun	1	Blade Chassis	2009
8	X6250 Blade	Sun	1	HRMS Reports	2009
9	X6250 Blade	Sun	1	HRMS T&D	2009
10	X6250 Blade	Sun	1	Antivirus Server	2009
11	X6250 Blade	Sun	1	SSP-DC-Mgmt	2009
12	X6250 Blade	Sun	5	SAP SERVER	2010
13	HCL Server	HCL	3	Not in Use	2006
14	SB6000 Blade Chassis	Sun	1	Blade Chassis	2011
15	SB X6270 M2 Blade	Sun	1	3i Infotech Web Services	2011
16	SB SPARC T3 Blade	Sun	1	HRMS Reporting Layer	2011
17	x4150	Sun	1	NET ADMIN	2009
Storage & Backup					
18	ST9990V	Sun	1	Sun-Storage	2009
19	SL500	Sun	1	Tape Library	2009
20	Brocade5100	Brocade	2	FC Switch	2009
21	Brocade 7500	Brocade	2	FCIP Router	2009
Desktops					
22	HP PC	PC	1	Solomon App Server	2004
23	PC-1	SUN PC	5	Onsite team	2009
24	Wipro Net	Wipro	1	HRMS Data Capturing	2010
Network & Security					
25	CISCO 6500-E	Cisco	2	Core Switch	2009
26	CISCO ASA 5580	Cisco	2	Firewall	2009
27	CISCO CATALYST 3750 G	Cisco	2	DMZ Switch	2009
28	Cisco IPS 4260	Cisco	2	IPS	2009
29	CISCO CATALYST 2950G	Cisco	1	L2 SWITCH	2009
30	CISCO ACE 4710	Cisco	2	SLB	2009

Bill of Material (Bengaluru):

Part No.	Description	Qty
	SUN 5120 Server	
SECAF142Z	SE T5120 BASE 8CORE 1.4GHZ	2
SESY9SD1Z	SE T5x20 T5x40 SW PRE-IN S106	2
X311L	NORTH AMERICAN/ASIA PWRCD RoHS	4
SESY2C1Z	SE 8GB FBDIMM (2*4GB) MEM	16
SG-PCIE2FC-QF4	4Gb FC Dual Port HBA	4
X3000A	RoHS-6 XVR-300 PCIEx8 Graphics	2
SESY9DV1Z	SE T5x20 DVD, 8X, RW	2
SECY9PS41Z	SE T5120 AC PSU 720W	4
SESY3C11Z	SE 146GB 10K RPM 2.5" SAS	4
SESY9MF1Z	Hard Disk Filler Panel	4
SESX9RK2Z	SE T5x20 EXPRESS RAIL KIT	2
SECY9BA1Z	SE T5120 4DISK HDD BKPLN	2
SECY9LS1Z	SE T5120 STD LABEL	2
	T2000	
T20-108B-32FA2C	SFT2000 8 Core 1.2 GHz, 4 Gb FC Dual Port HBA	2
	32 GB	2
	2*73 GB HDD	2
	V480	
SUN V480	SUN V480	1
	ULTRA TYPE SPARC III+1.2Ghz	1
	72 GB *2	1
	16 GB	1
	SUN M4000 (Backup Server)	
Config ID 7438109	Configuration: SEEPDCB2Z	1
SEEPDCB2Z	SE M4000 2.4GHz 2P32GB 2HDD	1
DOMAIN	Domain [1]	1
SG-XPCIE2FC-QF4	4Gb FC Dual Port HBA	2
X4447A-Z	Sun Quad GbE x8 PCIe card UTP	2
X7296A	RoHS-6 XVR-100 Graphics	1
SELX9P41Z	PWR CORD M4000-5000 125V	2
SEEX9FL1Z	SE_M4000 Filter Kit	1
X7281A-2	Sun PCI-E Dual GigE MMF	2
X7281A-2	Sun PCI-E Dual GigE MMF	2
	SUN SB 6000 Chassis	
A90-A	SB 6000 10U Base Chassis	1
X4621A	Dongle DB9 RJ45 2USB VGA	5
	PWR CORD, QTY 4, AC, 16A, EPAC	1
SG-XPCIE2FC-QB4-Z	SB6000 NEM 10-port GbE	2
X4250A	SB6000 CMM	1

Part No.	Description	Qty
	SUN Blade X6250 (DC, ADC, AV and SSP Server)	
A93-AA	SB X6250 Base Blade for XATO	4
4620A	SB REM RAID5 256MB cache	4
4401A	Sun Blade 2x2GB DDR2 FBDIMMs	5
RB-SS2CD-146G10KZ	146GB 10K RPM 2.5" SAS disk	10
X6250-AA-14M2500	X6250 CPU KIT E5420 (ATO)	8
X5075A-Z	Sun QGbE x8 PCIe EM	4
X7287A-Z	PCIe 4Gb FC 2P EM HBA, QLogic	4
	SUN Blade X6250 (SAP Servers)	
A93-AA	SB X6250 Base Blade for XATO	5
	2x4GB DDR 2	5
	146 GB SAS	20
	SB REM RAID5 256MB cache	5
	X6250 CPU KIT E5430 (ATO)	10
	Dual 4Gb FC Dual HBA	5
	SB 6000 Base Chassis	
UN-BLD6K-HS-OICL	SB 6000 10U Base Chassis	1
	SB 6000 10U Base Chassis with midplane with dongle and RJ45-Adapter	1
	PWR CORD, QTY 4, AC, 16A, EPAC	1
	Sun Blade X6270 M2 Server	
X-6270 M2	Sun Blade X6270 M2 Server	1
	4 GB RAM	4
	300 GB HDD	2
	E5620 4 core	2
	8Gb HBA	2
	Sun Blade T3-1B	
SUN-SPRCT3	Sun Blade T3-1B	1
	1.65 GHz 8 Core	1
	8 GB RAM	2
	300 GB HDD	2
	8 Gb FC HBA	2
	SUN 9990V Storage	
TV9DKC-F605I-146KS	ST9990V 146G/15k HDD Canister	144
TV9DKC-F605I-18	ST9990V Disk Array Frame	1
TV9DKC-F605I-300KM	ST9990V 300G15K HDDMultiVendor	24
TV9DKC-F610I-16FS	ST9990V Fibre 16Prt CHA-SWL4Gb	2
TV9DKC-F610I-1EC	ST9990V PwrCablKit 1Phase EUR	2
TV9DKC-F610I-1PS	ST9990 DKC AC Box Kit-1 Phase	2
TV9DKC-F610I-AB	ST9990 Additional Battery	1
TV9DKC-F610I-ABX	ST9990V Additional Battery-2	2
TV9DKC-F610I-C8G	ST9990V AddnlCacheMmry Mod8GB	5

Part No.	Description	Qty
TV9DKC-F610I-CX	ST9990V Cache Data Expan Kit	1
TV9DKC-F610I-DKA	ST9990V Back End Director(DKA)	2
TV9DKC-F610I-R1DC	ST9990V DEV I/F Cable Kt	1
TV9DKC-F610I-R1UC	ST9990V DEV I/F CableKt-3&4BED	1
TV9DKC-F610I-S4GQ	ST9990VShrdAddnlCacheMmryMd4GB	4
TV9DKC-F610I-SX	ST9990V Shared Memory Adapter	1
TV9DKC610I-5	ST9990V Disk Control Frame	1
TV9DKC-F605I-146K1	ST9990V146G/15k SprHDDCanister	4
TV9DKCF605I-300KM1	ST9990V 300G15KSPREMultiVendor	2
TV9044-220001-01	ST9900 BOS Ste Media Kit	1
TV9044-220001-03	ST9900 BOS Ste Base Lic	1
TV9044-220001-03D	ST9900 BOS Ste Above 25TB Lic	28
TV9044-220002-01	ST9900DisasterRecoveryMediaKit	1
TV9044-220002-03	ST9900DisasterRecovery Bse Lic	1
TV9044-220002-03A	ST9900DisasterRecvyUpto5TB Lic	1
TV9044-220004-01	ST9900 In-Sys Replctn Media Kt	1
TV9044-220004-03	ST9900 In-Sys Replctn Bse Lic	1
TV9044-220004-03B	ST9900 In-Sys ReplctnAbov5TBLc	10
TV9DKC-F605I-300KM	ST9990V 300G15K HDDMultiVendor	8
TV9044-220001-03D	ST9900 BOS Ste Above 25TB Lic	2
	SUN Tape Library SL500 LTO4	
	Configuration: SL500-30L4IB4GFZ	1
SL500-30L4IB4GFZ	SL500 30slotw/2IBMLTO4FC4G KEY	1
X-SL500K-DEM-W1/3Z	SL500 DEM w/ 1/3 slots KEY	1
PWRCORD10187061-Z	Cord,3X14AWG,15A,US/CAN,C13,3M	4
CABLE10800313-Z	FC, LC-LC, 50/125, Dplx, P,10M	8
XSL500-RED-PWR-Z	C/B, SL500 Redund power Supply	2
LTO4-IB4FC-SL500Z	LTO4 IBM FC 4Gb SL500 Dr	2
XSL500-TSOP-Z	C/B, SL500 touchscr op panel	1
X-SL500K-BASE30-50	SL500 30-50 slots-KEY	1
X-SL500K-1/3SLOTUP	SL500 1/3 DEM slots KEY	1
M-LTO4-LBPK-HOR	LTO4,800GB,LIB-PACK,HOR-LBL	1
	FC Switch & FCIP Router 7500 and 5100	
SG-XSWBRO-7500-Z	BrocadeSW7500 18Pt NoSFPs	2
SG-XSWBRO7500-FC-Z	Brocade7500FCIP SW License	2
X340L	SF 490/890 US Power Cords RoHS	4
XSFP-SW-4GB-4PK	4pk-4Gb FC transcvr short wave	4
SG-XSWBRO4100-AEB	Brocade5000/4100SW Pk-FW,APM,T	4
SG-XSWBROSFP1GE	Brocade 7500 Copper SFP	4
SG-XSWBRO5100-4NS	BROCADE 5100 WITH 4G SFP NO EB	2
SG-XSWBRO5100-POD4	Brocade 5100 POD WITH 4G SFP	2
SG-XSWBRO3X50-RK-Z	Brocade Std Switch Rack Kit	2

Part No.	Description	Qty
SG-XSWBRO-PWR-05-Z	Brocade Power Kit for Other	2
	Core Switch- Cisco 6500	
WS-C6509-E	Catalyst 6500 Enhanced 9-slot chassis,15RU,no PS,no Fan Tray	2
SV33AIK9-12233SXH	Cisco CAT6000-VSS720 IOS ADVANCED IP SERVICES SSH	2
VS-S720-10G-3C	Cat 6500 Supervisor 720 with 2 ports 10GbE and MSFC3 PFC3C	2
CF-ADAPTER-SP	SP adapter with compact flash for SUP720	2
MEM-C6K-CPTFL1GB	Catalyst 6500 Compact Flash Memory 1GB	2
WS-X6748-GE-TX	Cat6500 48-port 10/100/1000 GE Mod: fabric enabled, RJ-45	2
WS-F6700-DFC3B	Catalyst 6500 Dist Fwd Card, 256K Routes for WS-X67xx	2
WS-C6K-13SLT-FAN2	High Speed Fan Tray for Catalyst 6513 / Cisco 7613	2
WS-CAC-4000W-US	4000Watt AC Power Supply for US (cable attached)	4
VS-F6K-MSFC3	Catalyst 6500 Multilayer Switch Feature Card (MSFC) III	2
VS-F6K-PFC3C	Catalyst 6500 Sup 720-10G Policy Feature Card 3C	2
VS-S720-10G	Catalyst 6500 Supervisor 720 with 2 10GbE ports	2
BF-S720-64MB-RP	Bootflash for SUP720-64MB-RP	2
MEM-XCEF720-256M	Catalyst 6500 256MB DDR, xCEF720 (67xx interface, DFC3A)	2
WS-F6700-CFC	Catalyst 6500 Central Fwd Card for WS-X67xx modules	2
X2-10GB-SR	10GBASE-SR X2 Module	4
	Internet DMZ Switch - 3750	
WS-C3750G-24TS-E1U	Catalyst 3750 24 10/100/1000 + 4 SFP + IPS Image; 1RU	2
CAB-STACK-50CM	Cisco StackWise 50CM Stacking Cable	2
CAB-ACE	Power Cord Europe	2
	Cisco Redundant Power System	
PWR-RPS2300	Cisco Redundant Power System 2300 and Blower,No Power Supply	2
C3K-PWR-750WAC	Catalyst 3750-E / 3560-E 750WAC power supply	2
CAB-IND-10A=	10A Power cable for India	2
CAB-RPS2300-E	RPS2300 Cable for Catalyst 3750E/3560E and 2960 PoE Switches	2
BLNK-RPS2300	Bay Insert for Cisco Redundant Power System 2300	2
	Core Firewall (Cisco ASA 5580 at Intranet Zone)	
ASA5580-20-8GE-K9	ASA 5580-20 Appliance with 8 GE, Dual AC, 3DES/AES	2
CAB-SABS-C19-IND	SABS 164-1 to IEC-C19 India	4
ASA-VPN-CLNT-K9	Cisco VPN Client Software (Windows, Solaris, Linux, Mac)	2
ASA5580-4GE-CU	ASA 5580 4-Port 10/100/1000 Interface Card, RJ-45	2
Included: CAB-AC	Power Cord,110V	2
Included: SF-ASA5580-8.1-K8	ASA 5580 Series Software v8.1	2
Included: ASA5500-ENCR-K9	ASA 5500 Strong Encryption License (3DES/AES)	2
Included: ASA-ANYCONN-CSD-K9	ASA 5500 AnyConnect Client + Cisco Security Desktop Software	2
Included: ASA5580-PWR-AC	ASA 5580 AC Power Supply	2
	IPS at Intranet Zone	
IPS-4260-4GE-BP-K9	4260 Bundle with 4-Port Cu NIC	2
CAB-ACE	Power Cord Europe	2

Part No.	Description	Qty
IPS-SW-6.1	IPS Software version 6.1	2
IPS-4GE-BP-INT	4-Port Copper NIC with bypass for the IPS 4260 and 4270	2
	SLB at Intranet Zone	
ACE-AP-PAK	ACE Appliance License PAK	2
CAB-ACU	Power Cord UK	2
ACE-4710-1F-K9	ACE 4710 Hardware-1Gbps-5K SSL-500MbpsComp-5VC-50AppAccel	2
ACE-AP-SW-3.2	ACE Appliance SW 3.2	2
ACE-AP-1F-LIC	ACE 4710 1F License Bundle	2

13.7.2. Buy-Back Items: Vashi

S.N.	Model	Make	Qty	Purpose	Year of Purchase
Servers					
1	Sun-V490	Sun	1	Backup server	2007
2	SUN-V480	Sun	1	INLIAS Reporting	2004
3	SUN-E2900	Sun	2	INLIAS Reporting	2004
5	SE T5220	Sun	2	Mail server	2009
6	SUN-V480	Sun	1	Proxy server	2004
7	HCL 2700 CA	HCL	1	Trend Micro Control	2007
8	Sun Fire X4170 M2	Sun	1	CTA Server	2007
9	SUN-T5120	Sun	1	Web Portal server	2009
10	Sunblade6000 Chassis	Sun	1	Web Portal chassis	2009
11	SBT6320 Blade	Sun	7	Web Portal server Blade	2009
12	HCL 2700 BD	HCL	1	HCL helpdesk server	2007
13	Blade Chassis	HP	1	PC NOC	2004
14	Blade Server	HP	6	PC NOC	2004
15	HP DL580	HP	1	PC NOC	2004
16	Infiniti Global Line 2700ST	HCL	4	NOC server 1	2007
17	Infiniti Global Line 2700	HCL	1	SSP server	2007
18	HP ML 110	HP	1	FTP Server	2007
19	SUN-E2900	SUN	3	NOT IN USE	2004
Storage & Backup					
20	Silkworm 4100	Brocade	2	SAN switch A	2004
21	SUN-SL500	Sun	1	Tape Library	2007
22	Sun Tape Drive	Sun	2	DDS-4 tape drive	2004
23	SUN – L100	Sun	1	TAPE Library	2004
24	Half Height LTO-3	Quantum	1	External Tape Drive	2004
25	BrocadeSW7500	Brocade	2	FCIP Replication Router	2007
Network & Security					
26	Cisco-PIX 515 E	Cisco	2	DMZ Firewall	2004
27	Cisco 3750	Cisco	2	DMZ switch	2004
28	Cisco 6506	Cisco	2	Core switch	2004
29	Cisco 2950	Cisco	2	Management switch	2004
30	KVM switch		1	8 Ports KVM switch	2007
31	HCL-24TMS-2GCS	HCL	1	24 port switch	2007
32	Cisco ACE 4710	Cisco	2	SLB	2012
33	Cisco ASA 5585	Cisco	2	Core Firewall	2012
34	Cisco MCS 7800	Cisco	2	Call Manager	2004
Desktops					
35	Sun 150	SUN	1	Workstation	2004
36	HP MONITOR-5500	HP	1	Monitor	2005
37	MONITOR	Compaq	1	Monitor	2005

Bill of Material (Vashi):

Part No.	Description	Qty
	Backup Server - Sun-V490	
A52-CLZ4C216GTB	1.5 GHz Ultra SPARC IV+ Proc with 32 MB Cache	4
	512 MB DIMMs	32
	146 GB FC HDD	2
	2 * 1G / 6 * PCI slots / RPS	1
	SUN-V480	
SUN V480	SUN V480	2
	ULTRA TYPE SPARC III+1.2Ghz	2
	72 GB *2	2
	16 GB	2
	SUN-E2900	
SUN E2900	SUN E2900	5
	ULTRA TYPE SPARC IV	5
	72 GB *2	5
	64GB	5
	Web and Mail Server	
	Configuration: SEDPFJF2Z	1
SEDPFJF2Z	SE T5220 8CR 1.4GHZ 64GB 2X146	2
X320A	NO AMERICA/ASIA 220 PWR CRD KT	4
SG-XPCIE2FC-QF4	4Gb FC Dual Port HBA	4
X3000A	RoHS-6 XVR-300 PCIEx8 Graphics	2
X7281A-2	Sun PCI-E Dual GigE MMF	4
	Sunblade6000 Chassis	
A90-ASB 6000	Sunblade6000 10U Base Chassis	1
	SBT6320 Blade	
SNUX1437	1.2 GHz RISC Ultra SPARC T2, 8 Core	4
	16 GB RAM	4
	2 * 146 GB HDD	4
	SBT6320 Blade	
SNUX1437	1.2 GHz RISC Ultra SPARC T2, 8 Core	3
	8 GB RAM	3
	2 * 146 GB HDD	3
	T5120	
SNUX1443	RISC UltraSPARC T2, 1.2 GHz, 8 Core	1
	16 GB RAM	1
	2 * 146 GB , 2 * 73 GB	1
	HP Blade Chassis	
HP C7000	HP C7000 Blade Chassis	1
	HP Blade Server	
HP PROLIANT BL20P G3	HP PROLIANT BL20P G3	6
	2 INTEL XEON CPUS 3.2 GHZ	6
	1GB * 4 RAM	6
	72.8GB * 2 HDD	6
	X4150	
B13-AA	X4150 Base Chassis	1
	146 GB SAS	2
	8 Port-SAS HBA	1
	4 GB RAM	2

Part No.	Description	Qty
	7500 for Vashi	
SG-XSWBRO-7500-Z	BrocadeSW7500 18Pt NoSFPs	2
SG-XSWBRO7500-FC-Z	Brocade7500FCIP SW License	2
X340L	SF 490/890 US Power Cords RoHS	4
XSFP-SW-4GB-4PK	4pk-4Gb FC transcvr short wave	4
SG-XSWBRO4100-AEB	Brocade5000/4100SW Pk-FW,APM,T	4
SG-XSWBROSFP1GE	Brocade 7500 Copper SFP	4
	SL500 LTO3	
SL500-30L4IB4GFZ	SL500 30slotw/2IBMLTO4FC4G KEY	1
X-SL500K-DEM-W1/3Z	SL500 DEM w/ 1/3 slots KEY	1
PWRCORD10187061-Z	Cord,3X14AWG,15A,US/CAN,C13,3M	4
CABLE10800313-Z	FC, LC-LC, 50/125, Dplx, P,10M	8
XSL500-RED-PWR-Z	C/B, SL500 Redund power Supply	2
LTO4-IB4FC-SL500Z	LTO3 IBM FC 4Gb SL500 Dr	2
XSL500-TSOP-Z	C/B, SL500 touchscr op panel	1
X-SL500K-BASE30-50	SL500 30-50 slots-KEY	1
X-SL500K-1/3SLOTUP	SL500 1/3 DEM slots KEY	1
	Core Switch- Cisco 6500	
WS-C6509-E	Catalyst 6500 Enhanced 9-slot chassis,15RU,no PS,no Fan Tray	2
SV33AIK9-12233SXH	Cisco CAT6000-VSS720 IOS ADVANCED IP SERVICES SSH	2
VS-S720-10G-3C	Cat 6500 Supervisor 720 with 2 ports 10GbE and MSFC3 PFC3C	2
CF-ADAPTER-SP	SP adapter with compact flash for SUP720	2
MEM-C6K-CPTFL1GB	Catalyst 6500 Compact Flash Memory 1GB	2
WS-X6748-GE-TX	Cat6500 48-port 10/100/1000 GE Mod: fabric enabled, RJ-45	2
WS-F6700-DFC3B	Catalyst 6500 Dist Fwd Card, 256K Routes for WS-X67xx	2
WS-C6K-13SLT-FAN2	High Speed Fan Tray for Catalyst 6513 / Cisco 7613	2
WS-CAC-4000W-US	4000Watt AC Power Supply for US (cable attached)	4
VS-F6K-MSFC3	Catalyst 6500 Multilayer Switch Feature Card (MSFC) III	2
VS-F6K-PFC3C	Catalyst 6500 Sup 720-10G Policy Feature Card 3C	2
VS-S720-10G	Catalyst 6500 Supervisor 720 with 2 10GbE ports	2
BF-S720-64MB-RP	Bootflash for SUP720-64MB-RP	2
MEM-XCEF720-256M	Catalyst 6500 256MB DDR, xCEF720 (67xx interface, DFC3A)	2
WS-F6700-CFC	Catalyst 6500 Central Fwd Card for WS-X67xx modules	2
X2-10GB-SR	10GBASE-SR X2 Module	4
	SLB at Intranet Zone	
ACE-AP-PAK	ACE Appliance License PAK	2
CAB-ACU	Power Cord UK	2
ACE-4710-1F-K9	ACE 4710 Hardware-1Gbps-5K SSL-500MbpsComp-5VC-50AppAccel	2
ACE-AP-SW-3.2	ACE Appliance SW 3.2	2
ACE-AP-1F-LIC	ACE 4710 1F License Bundle	2

13.8 Annexure 8: Hardware Sizing for Mail Messaging Solution

Server Sizing:

S.N.	Server Type	Qty	Detail of Number of Processors with Cores	RAM	Internal HDD	Operating System

Storage Sizing (in Terabyte):

S.N.	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6
SAS Storage Required for Mail Messaging						
SATA Storage Required for Mail Archiving						

13.9 Annexure 9: Power Details for Proposed Hardware

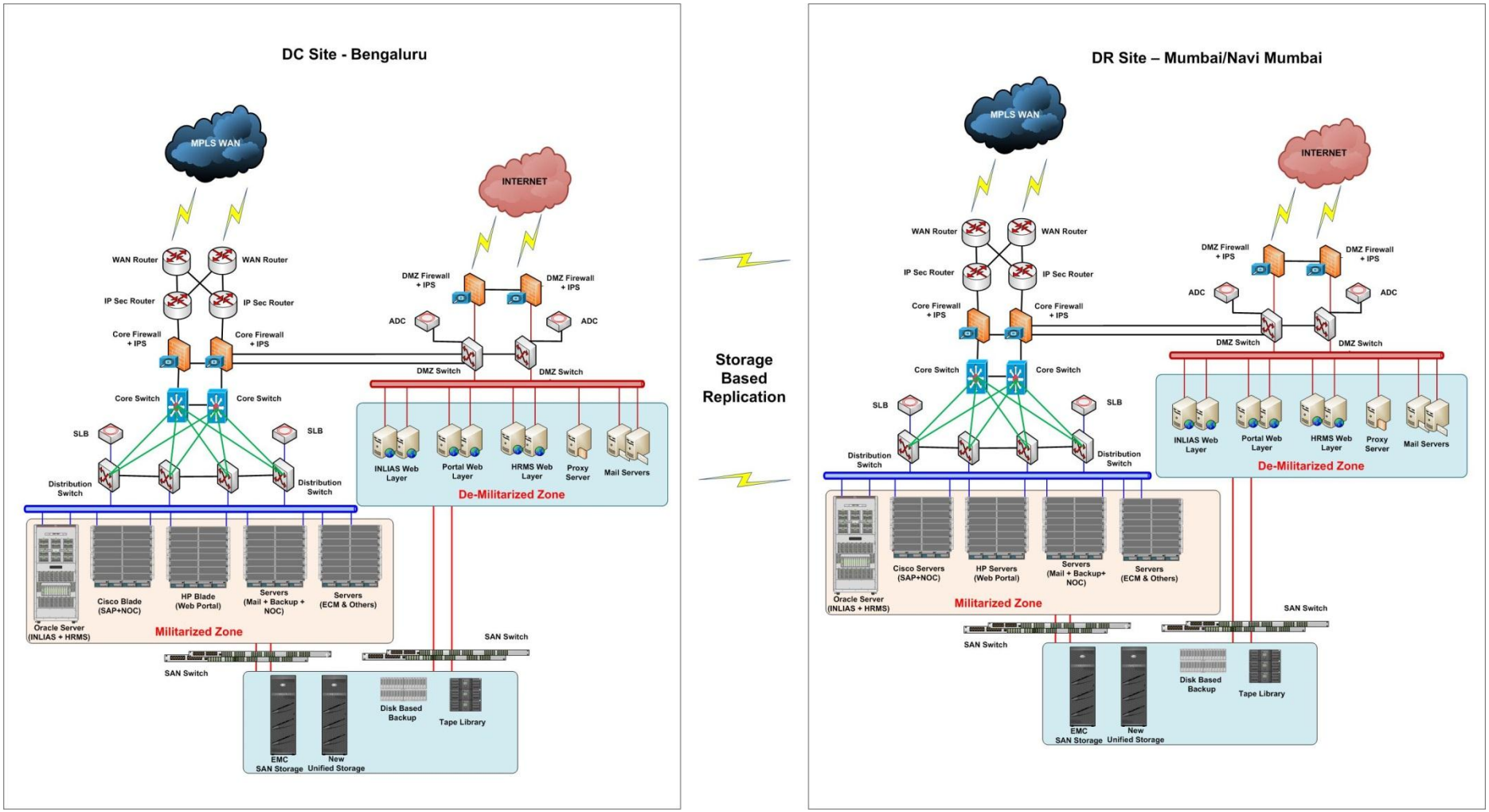
DC Site:

Solutions	Make & Model	Unit Power (KVA)	Qty	Total Power (KVA)
Enterprise Storage System			1	
SAN Switch			2	
FC-IP Routers			2	
Tape Library			1	
Disk Based Backup Solution			1	
Blade Chassis with Proposed Servers				
Core Switch			2	
DMZ Switch			2	
Distribution Switch			4	
Core Firewall with Integrated IPS			2	
DMZ Firewall with Integrated IPS			2	
Server Load Balancer			2	
Application Delivery Controller			2	
Any Other, (Please specify)				

DR Site:

Solutions	Make & Model	Unit Power (KVA)	Qty	Total Power (KVA)
Enterprise Storage System			1	
SAN Switch			2	
FC-IP Routers			2	
Tape Library			1	
Disk Based Backup Solution			1	
Blade Chassis with Proposed Servers				
Core Switch			2	
DMZ Switch			2	
Distribution Switch			4	
Core Firewall with Integrated IPS				
DMZ Firewall with Integrated IPS			2	
Server Load Balancer			2	
Application Delivery Controller			2	
Any Other, (Please specify)				

13.10 Annexure 10: Proposed DC-DR Layout



13.11 Annexure 11: Application Framework

S.N.	Application	DC Location	DR Location	Current State	To be State	Role	Responsibility
1	INLIAS	Bengaluru	Mumbai	1. Currently INLIAS is running on Oracle Servers (Solaris Platform) 2. OICL is in process of refreshing the existing hardware for INLIAS through separate RFP Process.	Oracle M6 Server	Operating System installation, hardening	Oracle SI
						Application Migration	3i Infotech
						Database Migration	3i Infotech
						Server hardware	Oracle SI
						LAN Integration	Bidder
						Storage Migration & Integration	Bidder
						Backup data and restoration	Oracle SI
						Validation of INLIAS– Post Migration • App • DB • Backup-restore	3i Infotech
2	HRMS	Bengaluru	Mumbai	1. OICL is in process of refreshing existing hardware for HRMS through separate RFP Process. 2. Currently INLIAS is running on Oracle Servers (Solaris Platform)	Oracle M6 Server	Operating System installation, hardening	Oracle SI
						Application Migration	Wipro
						Database Migration	Wipro
						Server hardware	Oracle SI
						LAN Integration	Bidder
						Storage Migration & Integration	Bidder
						Backup data and restoration	Oracle SI
						Validation of HRMS solution – Post Migration • App • DB • Backup-Restore	Wipro
3	Web Portal	Bengaluru	Mumbai	OICL is revamping its existing web portal and has selected PwC for this activity.	HP c7000 Chassis	Operating System installation, hardening	NA
						Application Migration	NA
						Database Migration	NA
						Server hardware	Wipro

S.N.	Application	DC Location	DR Location	Current State	To be State	Role	Responsibility
				Currently PwC is migrating the web portal from exiting platform to new platform.		Logistic and shipment	Bidder
						Transit insurance	Bidder
						LAN Integration	Bidder
						Storage Migration & Integration	Bidder
						Backup data and restoration	Bidder
						Application continuity check and validation	PWC
						Validation of Portal solution – Post Migration • App • DB • Backup-Restore	PWC
4	SAP	Mumbai	Bengaluru	Currently SAP is being managed by M/s Aegis. SAP is running on Cisco Blade Servers (Windows Platform) supplied and being supported by M/s Sify.	Cisco USC Chassis	Application Ownership	Aegis
						Application Migration	NA
						Database Migration	NA
						Server hardware	Sify
						Logistic and shipment	Bidder
						Transit insurance	Bidder
						LAN Integration	Bidder
						Storage Migration & Integration	Bidder
						Backup data and restoration	Bidder
						Application continuity check and validation	Aegis
						Validation of SAP solution – Post Migration • App • DB • Backup-Restore	Aegis
5	EMS, Anti-Virus, Active	Mumbai	Bengaluru	HCL Infosystems Ltd shall implement the EMS, AV,	Cisco USC Chassis	Application Ownership	HCL Infosystems
						Application Migration	NA

S.N.	Application	DC Location	DR Location	Current State	To be State	Role	Responsibility
	Directory & Help desk			AD and Helpdesk solution on Cisco UCS Chassis.		Database Migration	NA
						Server hardware	HCL Infosystems
						Logistic and shipment	Bidder
						Transit insurance	Bidder
						LAN Integration	Bidder
						Storage Migration & Integration	Bidder
						Backup data and restoration	Bidder
						Application continuity check and validation	HCL Infosystems
						Validation of NOC solution – Post Migration • App • DB • Backup-Restore	HCL Infosystems
6	Mail Messaging	Mumbai	Bengaluru	SUN one Mail-Messaging Solution.	Bidder to Propose	Application Ownership	Bidder
						Application Migration	Bidder
						Database Migration	Bidder
						Server hardware	Bidder
						LAN Integration	Bidder
						Storage Migration & Integration	Bidder
						Backup data and restoration	Bidder

-End of Document-