

The Oriental Insurance Company Limited

Head Office, New Delhi



Request for Proposal

For

Selection of Vendor for Supply, Installation and Maintenance of Desktop & IT Services Management Solution (DITSM) including Active Directory, Antivirus and Helpdesk Solution

(Tender Reference No.: OICL/HO/ITD/DITSM/2022/01 Dated 09/12/2022)

Information Technology Department

The Oriental Insurance Company Limited
NBCC Office Complex, East Kidwai Nagar
2nd Floor, Office Block 4,
New Delhi- 110023

CIN- U66010DL1947GOI007158
www.orientalinsurance.org.in



**This page is
Intentionally
Left blank**

Non-Refundable Tender Fee

Non-Transferable Receipt

To be filled by OICL Official

Tender Ref. No.	OICL/HO/ITD/DITSM/2022/01
Date of Issue	
Tender Issued to Bidder	



Draft No.	
Date	
Draft Amount	
Bank Name	
Name of OICL Official	
Designation of OICL Official	
Signature	
OICL Official	Bidder's Representative with Contact No. and Date



**This page is
Intentionally
Left blank**



Non-Refundable Tender Fee

Non-Transferable Receipt

To be filled by OICL Official

Tender Ref. No.	OICL/HO/ITD/DITSM/2022/01
Date of Issue	
Tender Issued to Bidder	
Draft No.	
Date	
Draft Amount	
Bank Name	
Name of OICL Official	
Designation of OICL Official	
Signature	
OICL Official	Bidder's Representative with Contact No. and Date

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.

Copyright © 2022 The Oriental Insurance Company Limited.

Contents

1 Introduction	12
1.1 About the Company	12
1.2 Notice Inviting Bids	12
1.3 Project Objective	12
1.4 Schedule of Events	13
1.5 Availability of tender document	15
1.6 Eligibility Criteria	15
1.7 Project Timelines	17
1.8 Escalation Matrix	17
1.9 Contract Period	17
2 Scope of Work	18
2.1 Background & Current IT Infrastructure	18
2.2 Existing Inventory	18
2.3 Detailed Scope of Work	19
2.3.1 Sizing of Hardware	19
2.3.2 Upgrade of Active Directory	19



2.3.3 Antivirus Solution with EDR Functionality	21
2.3.4 Enterprise Management System.....	22
2.3.5 Helpdesk Solution	23
2.3.6 OEM's Scope	24
2.3.7 Facilities Management (FM) & Annual Technical Support (ATS)	25
2.3.8 Project Management.....	28
2.3.9 Transition Management	28
2.3.10 Training.....	29
2.3.11 Documentation.....	29
2.3.12 Reporting	29
2.3.13 Escrow	30
2.4 Geographical Location.....	30
3 Terms & Conditions	31
3.1 General	31
3.1.1 Definitions	31
3.1.2 Amendment to Bid Document.....	31
3.1.3 Sub-contracts	32
3.1.4 Conditional bids.....	32
3.1.5 Submission of Bids	32
3.1.6 Performance Security	32
3.1.7 Pre-Bid Meeting.....	32
3.1.8 Delay in Bidder's performance	33
3.1.9 Payment Terms	33
3.1.10 Mode of Payment	34
3.1.11 Penalties and delays in Bidder's performance	34
3.1.12 Currency of Payments	34
3.2 Other RFP Requirements	34
4 Terms of Reference ('ToR').....	35
4.1 Contract Commitment.....	35
4.2 Completeness of Project.....	35
4.3 Compliance	35
4.4 Assignment	35
4.5 Canvassing/Contacting	36
4.6 Indemnity.....	36
4.7 Inspection of Records.....	36
4.8 Publicity	36
4.9 Solicitation of Employees.....	36
4.10 Information Ownership	37
4.11 Sensitive Information	37
4.12 Technological Advancements	37



4.13 Confidentiality	37
4.14 Force Majeure	38
4.15 Termination for Default	38
4.16 Liquidated Damages	38
4.17 Termination for Insolvency	38
4.18 Termination for Convenience	39
4.19 Resolution of disputes	39
4.20 Governing Language	40
4.21 Applicable Law	40
4.22 Prices	40
4.23 Taxes & Duties	40
4.24 Deduction	40
4.25 No Claim Certificate	40
4.26 Cancellation of the contract & compensation	40
4.27 Rights reserved by OICL	41
4.28 Limitation of Liability	41
4.29 Waiver	41
4.30 Violation of terms	41
4.31 Adherence to Terms and Conditions	42
4.32 Integrity Pact	42
4.33 Outsourcing Agreement	42
4.34 Regulations, Legal & Compliance	43
4.35 Guidelines for MSME	44
4.36 Transfer of Title	44
5 Instruction to Bidders	44
5.1 Instructions for Online Bid Submission	44
5.2 Tender Bidding Methodology	44
5.3 Bid Security	45
6 Bid Documents	45
6.1 Eligibility Bid Documents	45
6.2 Technical Bid Documents	45
6.3 Commercial Bid Documents	46
6.4 Eligibility cum Technical Evaluation	46
6.5 Commercial Evaluation	48
7 Service Level Agreement	49
7.1.1 Service Level Agreement and Targets	49
7.1.2 Service Level Measurement	50
7.1.3 Availability	50
7.1.4 Management, Reporting and Governance	51
7.1.5 Support/ Maintenance Matrix	52
7.1.6 Exception	52
8 Disclaimer	53



9 Annexure	53
9.1 Annexure 1: Application form for Eligibility Bid	54
9.2 Annexure 2: Technical Experience Details and Reference Form.....	55
9.3 Annexure 3: Contract Form.....	55
9.4 Annexure 4: Query Format	58
9.5 Annexure 5: Bid Security Declaration	59
9.6 Annexure 6: Pro forma for Performance Security.....	59
9.7 Annexure 7: Statement of No Deviation	60
9.8 Annexure 8: Office locations and service infrastructure facilities	61
9.9 Annexure 9: Bidder Profile	62
9.10 Annexure 10: Undertaking for providing authorized representatives of IRDAI the right to inspection, investigation, obtaining information	62
9.11 Annexure 11: Non-Disclosure Agreement.....	63
9.12 Annexure 12: Integrity Pact.....	68
9.13 Annexure 13: Undertaking of Authenticity for Appliance and Equipment Supplies	74
9.14 Annexure 14: Manufacturers Authorization Format	75
9.15 Annexure 15: Undertaking from OEM for Equipment Supplies on time.....	76
10 Appendix.....	76
10.1 Appendix 1: Technical Specifications.....	76
10.2 Appendix 2: Commercial Bill of Material	110



Purpose of this Document

The purpose of this Request for Proposal (hereafter referred to as “RFP”) is to define scope of work for the selection of Vendor for Supply, Installation and Maintenance of Desktop & IT Services Management Solution (DITSM) including Active Directory, Antivirus and Helpdesk Solution.

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

Definitions and Acronyms

AMC	Annual Maintenance Contract
ATS	Annual Technical Support
Bidder	Single point appointed by OICL for this RFP
CVC	Central Vigilance Commission
DC	Data Centre
DRS/DRC/DR	Disaster Recovery Site
HO	Head Office
RO	Regional Office
DO / BO / SVC	Divisional Office / Branch Office / Service Centre
EC / MO	Extension Counter / Micro Office
INR	Indian Rupees
IP	Internet Protocol
IT	Information Technology
LAN	Local Area Network
Mbps	Million Bits per Second
MPLS	Multi-Protocol Label Switching
PO	Purchase Order
OEM	Original Equipment Manufacturer
OICL	The Oriental Insurance Company Limited
OS	Operating System
RFP	Request for Proposal
SOW	Scope of Work
T&C	Terms & Conditions
TCO	Total Cost of Ownership
TO	Technical Offer
ToR	Terms of Reference
UAT	User Acceptance Test
SME	Subject Matter Expert



VAPT	Vulnerability Assessment and Penetration Testing
SIEM	Security Information and Event Management
BFSI	Banking, Financial Institution and Insurance Company
POC	Proof of Concept
MSME	Micro, Small, Medium Enterprises
NSIC	National Small Industries Corporation
ISO	International Organization for Standardization
GST	Goods and Service Tax

PAN	Permanent Account Number
HRMS	Human Resource Management System
Kbps	Kilobytes per second
NOC	Network Operations Centre
SOC	Security Operations Centre



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 and Secondary Data Centre (SDC/DR) at Navi Mumbai, 29 Regional offices in various cities, Oriental Staff Training College (OSTC) at Faridabad, 450+ divisional offices, 500+ branch offices, Regional Training Centers, 30+ Claims Service centers, 30+ TP Hubs and 700+ Business Centers/micro offices geographically spread out across India. Currently head office has 4 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 BCs 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 Bengaluru and Navi Mumbai. 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 10 million new policies in the year 2020-21. 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 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 online bids from eligible Bidders for Supply, Installation and Maintenance of Desktop & IT Services Management Solution (DITSM) including Active Directory, Antivirus and Helpdesk Solution.

1.3 Project Objective

The Oriental Insurance Company Ltd. (OICL) envisages to select a competent bidder for Supply, Installation and Maintenance of Desktop & IT Services Management Solution (DITSM) including Active Directory, Antivirus and Helpdesk Solution for a period of 6 years.

OICL currently has approximately 13,000 desktops in its offices all over India. OICL intends to upgrade the Active Directory Solution for all desktops available across country at OICL. In order to manage these desktops OICL intends to have an Enterprise Management Software. Also OICL wants to implement an anti-virus solution with EDR on these desktops and Servers available at DC & DR Site. OICL requires the bidder to establish and maintain



a Help Desk to service, track and route requests through phone / e-mail or any other media related to the solutions and Infrastructure proposed by the Bidder as a part of this RFP.

OICL reserves to right to ask any or all Bidders to conduct Proof of Concept (POC). Unsuccessful POC will lead to disqualification of bidder(s).

1.4 Schedule of Events

General Details	
Department's Name	Information Technology Department
Scope of Work	Selection of Vendor for Supply, Installation and Maintenance of Desktop & IT Services Management Solution (DITSM) including Active Directory, Antivirus and Helpdesk Solution
Tender Details	Request for proposal for Selection of Vendor for Supply, Installation and Maintenance of Desktop & IT Services Management Solution (DITSM) including Active Directory, Antivirus and Helpdesk Solution
Tender Type	Open
Tender No.	OICL/HO/ITD/DITSM/2022/01
Consortium	Not Allowed
Download Tender Documents	Tender Document can be downloaded from OICL's website- https://orientalinsurance.org
Key Dates	
Document Purchase Start Date	09/12/2022
Document Purchase End Date and Time	06/01/2023, 3:00 PM
Last Date and Time for receipt of prebid queries	16/12/2022, 3:00 PM
Pre-Bid Meeting Date, Time and Location*	19/12/2022, 3:00 PM
Last Date and Time for submission of Bids	06/01/2023, 3:00 PM
Date and Time of Eligibility cum Technical Bid Opening	06/01/2023, 3:30 PM
Presentation by Qualified Bidders	Will be communicated
Opening of Commercial bid	Will be communicated
Declaration of L1 Bidder	Will be communicated
Payment Details	



Tender Fees (INR)	<p>INR 10,000 (Rupees Ten Thousand only) by crossed Demand Draft/Banker's Pay Order/ Online transfer in favour of "The Oriental Insurance Company Limited" payable at New Delhi. The RFP Document Price is non-refundable and inclusive of taxes. In case of Online transfer:</p> <table border="1" data-bbox="655 488 1479 969"> <tr> <td>Name of Bank A/c (i.e., beneficiary)</td><td>The Oriental Insurance Company Limited</td></tr> <tr> <td>Name of the Bank</td><td>UCO Bank</td></tr> <tr> <td>Address of the Bank</td><td>4/2B, Asaf Ali Road Near Delite Cinema, New Delhi – 110002</td></tr> <tr> <td>Bank Branch Name</td><td>Asaf Ali Road</td></tr> <tr> <td>Account type</td><td>Current</td></tr> <tr> <td>Account No</td><td>01150200000009</td></tr> <tr> <td>IFSC Code</td><td>UCBA0000115</td></tr> <tr> <td>Nine-digit MICR Code No</td><td>110028003</td></tr> </table> <p><i>(Exempt for eligible entities (i.e., MSME/NSIC), as per Government of India Guidelines, subject to submission of the relevant certificate.</i></p>	Name of Bank A/c (i.e., beneficiary)	The Oriental Insurance Company Limited	Name of the Bank	UCO Bank	Address of the Bank	4/2B, Asaf Ali Road Near Delite Cinema, New Delhi – 110002	Bank Branch Name	Asaf Ali Road	Account type	Current	Account No	01150200000009	IFSC Code	UCBA0000115	Nine-digit MICR Code No	110028003
Name of Bank A/c (i.e., beneficiary)	The Oriental Insurance Company Limited																
Name of the Bank	UCO Bank																
Address of the Bank	4/2B, Asaf Ali Road Near Delite Cinema, New Delhi – 110002																
Bank Branch Name	Asaf Ali Road																
Account type	Current																
Account No	01150200000009																
IFSC Code	UCBA0000115																
Nine-digit MICR Code No	110028003																
General Details																	
	<i>Certificate shall be valid on the date of Bid Submission)</i>																
EMD Amount (INR)	Bid Security Declaration as per format provided in Annexure 5 to be submitted																
Bid Validity	As per Tender Document																
Performance Bank Guarantee (For successful Bidder)	As per Tender Document																
Other Details																	
Mode of Tender	Online																
Contact details of e-Tender service provider	GeM Portal																
Contact Information	<p>Deputy General Manager Information Technology Department, The Oriental Insurance Company Limited NBCC Office Complex, East Kidwai Nagar, 2nd Floor, Office Block 4, New Delhi- 110023 E-mail: tender@orientalinsurance.co.in</p>																

**It is mandatory for the Bidder to purchase the tender document so as to participate in the pre-bid meeting.*

**The Pre-bid meeting will be held via video-conferencing and link for the same will be available on the day of meeting on OICL's Web Portal (<https://orientalinsurance.org.in>) under tender section.*



1. 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.
2. 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

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, NBCC Office Complex, East Kidwai Nagar, 2nd Floor, Office Block 4, New Delhi- 110023

The RFP document will be available for sale at the above address on all working days as per the date and time specified in section 1.4 Schedule of Events on payment of non-refundable Tender Fee of Rs. 10,000/- (Rupees Ten Thousand only) (Exempt for eligible entities (i.e., MSME/NSIC), as per Government of India Guidelines, subject to submission of the relevant certificate. Certificate shall be valid on the date of Bid Submission) by crossed Demand Draft/ Banker's Pay Order/ Online Transfer in favor of "The Oriental Insurance Company Limited" payable at New Delhi. **Tender fee is inclusive of all taxes.**

In case of Online transfer, requisite details are provided in the table above- 1.4: Schedule of Events

A Copy of the Tender document is available on the web portal <https://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

#	Eligibility Criteria	Documents Required
1	The bidder should be a Government Organization/ PSU/ or a Public Limited Company/ Private Limited Company under companies act 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 (not inclusive of the turnover of associate companies) in last three financial years (2019-20, 2020-21 and 2021-22).	1. Audited Financial statements for the respective financial years and/or 2. Published Balance Sheet and/or 3. CA Certificate
4	The Bidder should have a positive net worth in the last three financial years (2019-20, 2020-21 and 2021-22).	
5	Bidder must have valid ISO 9001: 2015 & ISO/IEC 27001:2013 ISO 20001 certificates on the date of submission of bid	Copy of relevant certifications
6	The Bidder should not be blacklisted by any Government or PSU enterprise in India as on the date of the submission of bid.	Self-Declaration letter by Bidder authorized signatory.



7	The Bidder should hold a valid GST Number & PAN Card and should be registered with the appropriate authorities for all applicable statutory taxes/duties.	1. Copy of GST certificate to be submitted 2. Copy of PAN Card to be submitted
8	The bidder/OEM should have its own Support and Services Center based in Bengaluru and Mumbai.	Self-Declaration on bidder letter head duly signed and stamp
9	The Bidder should be Original Equipment Manufacturer (OEM) or its Authorized reseller/seller or partner of the products offered	A valid Manufacturer Authorization Form from the OEM as per Annexure 14
10	Bidder should have supplied, implemented and provided/ providing maintenance services for following solution in last five (5) years. a) Proposed EMS solution in a BFSI/PSU/Government Organization in India with at least 7,500 employees b) Endpoint Security with at least 7,500 endpoints in a BFSI/PSU/ Government Organization in India c) AD Upgrade/ Implementation in a BFSI/PSU/Government Organization in India	Credential Letter OR Copy of Purchase Order/ Contract copy along with Sign off/ completion letter
OEM's Credentials		
11	The proposed Enterprise Management System should have been implemented in at least one Scheduled Commercial Bank/ Insurance Company / PSU/ Govt. Organization in India with at least 7,500 employees	Credential Letter OR Copy of Purchase Order/ Contract copy along with Sign off/ completion letter
12	The proposed Endpoint Security should have been implemented/ under implementation in at least one Scheduled Commercial Bank/ Insurance Company / PSU/ Govt. Organization in India with at least 7,500 endpoints	Under Implementation Projects: Copy of Purchase Order/ Contract Implemented Projects: Credential Letter OR Copy of Purchase Order/ Contract copy along with Sign off/ completion letter

*OICL reserves the right to verify references provided by the Bidder independently. Any decision of OICL in this regard shall be final, conclusive and binding up on the bidder. OICL may accept or reject an offer without assigning any reason whatsoever.

Note:

1. Bidders need to ensure compliance to all eligibility criteria points.
2. In-case of corporate restructuring, the earlier entity's incorporation certificate, financial statements, Credentials, etc. may be considered.
3. In case of business transfer where Bidder has acquired a Business from an entity ("Seller"), work experience credentials of the Seller in relation to the acquired business may be considered.



4. Purchase orders without relevant organization confirmation through a credential letter will not be considered as credentials (as applicable).
5. If an agent submits a bid on behalf of the Bidder/ OEM, the same agent shall not submit a bid on behalf of another Principal/ OEM for the same solution.
6. While submitting the bid, the Bidder is required to comply with inter alia the following CVC guidelines detailed in Circular No. 03/01/12 (No.12-02-6 CTE/SPI (I) 2 / 161730 dated 13.01.2012): 'Commission has decided that in all cases of procurement, the following guidelines may be followed:
 - a. *In RFP, either the Indian agent on behalf of the Bidder/OEM or Bidder/OEM itself can bid but both cannot bid simultaneously for the same item/product in the same RFP. The reference of 'item/product' in the CVC guidelines refer to 'the final solution that bidders will deliver to the customer.'*
 - b. *If an agent submits a bid on behalf of the Bidder /OEM, the same agent shall not submit a bid on behalf of another Bidder /OEM in the same RFP for the same item/product.'*

1.7 Project Timelines

The Project Manager/Coordinator shall submit a weekly report on the progress of the project to OICL and appraise the activities completed during the week and activities to be taken up in the upcoming week. Necessary assistance from OICL officials will be provided to ensure that activities are completed in time. The detailed activities to be completed in each phase are mentioned below along with the timelines.

After complete implementation of the Solution as defined in Scope of Work, OICL shall monitor the performance of the Solution for a period of ONE month. The said period will be treated as Evaluation Period and the Project closure process shall be initiated by OICL only post satisfactory performance of the Solution and the sign off of the Project shall take place.

#	Activity	Time Period for Completion
1	Active Directory Upgrade	T+1.5 months
2	Anti-Virus with EDR	T+2 months
3	Enterprise Management System	T+3 months
4	Helpdesk Solution	T+3 months

**T is the date of acceptance of PO*

1.8 Escalation Matrix

OICL as well as the Bidder will decide an escalation matrix to resolve any issues that may crop up during the project period. Both OICL and the Bidder shall inform the names of the persons, designation, Email ids and their telephone numbers for the escalation matrix to be effective.

1.9 Contract Period

The term of the Contract shall be for a period of 6 years from the date of issuance of purchase order and further extendable up to one more year on mutually agreed terms between OICL and Bidder.



2 Scope of Work

2.1 Background & Current IT Infrastructure

OICL's IT Infrastructure is enabled by a 24x7 data centre. Within the data centre, various servers and associated equipment are hosted that provide the processing power and storage for manning/managing application programs. This layer also includes system softwares (operating system) that forms a part of the hardware deployed.

The servers in turn are used to host applications including INLIAS, SAP, HRMS, Portal, E-mail, Proxy, etc. that provide business services to the users.

On top of the application layer there is a network layer that makes these applications accessible from remote offices (VPN) and finally the end user's computer (LAN).

The users accessing these applications from their desktops form the top of this logical view of OICL's IT landscape. All other elements are ultimately to serve the users in performing their business functions.

2.2 Existing Inventory

□ Existing Desktop Inventory

- OICL has approximately 13,000 desktops across all offices in the country.
- The Operating Systems on these Desktops is Windows 8 and Windows 10

□ Existing Active Directory

- The existing Active Directory Solution is on Microsoft Windows 2012 Standard R2. ○ Currently OICL is having 13,000 Client Access Licenses.

□ Existing Anti-Virus System

- OICL is using Symantec Anti-virus Licenses on all desktops. ○ Currently OICL is having 13,000 perpetual Antivirus Licenses with Gold Support.

□ Bandwidth Details

- Most of OICL's Offices are connected to data centre through MPLS VPN Dual Active-Active Link. Few offices are connected to VPN though secure Roam Connect over Internet. ○ The following table specifies the bandwidth available at various OICL offices:

Office	Bandwidth
RO	4 Mbps (Dual Active-Active)
DO	512 Kbps/ 1 Mbps (Dual Active-Active)
BO	384 Kbps (Dual Active-Active)
EC / MO	128 Kbps/ 256 Kbps
SVC	1 Mbps/ 2 Mbps (Dual Active-Active)
TP Hub	384 Kbps- 1 Mbps (Dual Active-Active)
HO	20 Mbps (Dual Active-Active)



Bidder to ensure that solution is designed as per bandwidth details mentioned above. No extra bandwidth will be provided.

Bidder to note that OICL is in the process of upgrading its Bandwidth. Requisite details will be shared once it is finalized.

□ **Existing DC-DR Details**

- Currently OICL has its Data Center Site at Bengaluru and Disaster Recovery Site at Rabale (Navi-Mumbai).
- For Active Directory, Antivirus, Enterprise Management Software & Helpdesk Solution, OICL will treat Rabale as DC Site and Bengaluru as DR Site.

2.3 Detailed Scope of Work

The scope of this project includes upgrade of Active Directory & Supply, Installation and Maintenance of Antivirus, Enterprise Management Software, Helpdesk Solution for a period of 6 years.

Bidder to ensure that adequate support from OEM is factored during and post implementation for the entire contract duration.

2.3.1 Sizing of Hardware

OICL will provide OS, VMs & Storage only. Bidder is required to propose the sizing of the VMs required for successful operationalization of all solutions. Any other component like cluster license, resilient storage Licenses or other equivalent licenses & any other hardware/ software licenses required should be factored by the Bidder.

The proposed solution should be in HA at DC & DR.

For machines connected to VPN through Internet, Reporting has to be managed through server hosted in DMZ at data center. Bidder has to share hardware sizing & OS details for this server. Bidder shall also be responsible to supply database & other licenses/ hardware required to run the solution.

The bidder shall propose hardware (only from the sizing perspective) such that at any point in time during the contract period, the average CPU utilization should not exceed 70% at the primary data center and Disaster Recovery Center. In case, the utilization exceeds 70%, Bidder will be responsible for augmentation at no additional cost to OICL.

2.3.2 Upgrade of Active Directory

The existing active directory is implemented on Windows 2012 Standard R2 Server. The Bidder shall be responsible for upgrade of Single Active Directory Domain using latest Platform with High Availability and manage all desktops/Servers at all the Branches and offices across the country with a single domain and to have a Standard Operating Environment rolled out across its desktops and laptops. The activity also includes setting up Group policies and all the necessary Windows components as per Microsoft best practices. Bidder is required to maintain the AD setup for the tenure of the contract. The Bidder's scope of work for active directory services is as follows:

1. For the current requirement, the number of users to be considered is 10,000.



2. The Active Directory solution should be implemented at DC, DRC and RO, HO, branches and other office locations of OICL. AD data should be replicated at DRC. In case of a disaster at DC, all branches should seamlessly connect/authenticate with AD at DRC.
3. DR solution should be 100% of DC Configuration. In case OICL plans for a separate replica of AD Solution for integration of AD with some other services of OICL, Bidder has to manage that infrastructure as well.
4. The Bidder should develop a project plan for implementation of AD services indicating milestones and deliverables to OICL. Bidder is expected to size the solution basis the bandwidth details provided by OICL for DC and DRC replication of AD data to be in sync with each other.
5. Design & implement the logical and physical structure of Directory services, Organization Unit.
6. Design and implementation of group policy, domain policy, naming conventions of the organization's unit as per OICL's requirement as well as industry best practices.
7. Bidder should provide the complete Group policy settings for user, computer and servers. Bidder is required to propose and implement various policies such as password policy, power management policy, device policy, backup policy, software policy, access rights to the users and groups etc. Bidder will also be responsible for providing reports of all desktops for deployment of AD policies periodically.
8. The Bidder shall be responsible for User, Machine (Laptop/Desktop) & User Migration to new Active Directory Domain from the existing Domains without any disruption in day-to-day work.
9. Bidder is required to evaluate the business requirements for AD Migration and perform an audit on the existing AD infrastructure to verify its health.
10. Bidder should provide the approach for joining of desktops/ laptops across the country to the domain. Desktops joining to OICL domain and user profile migration in Desktops shall be done by OICL's AMC partner. However, if any issue arises with the domain, the Bidder's resource shall be responsible to coordinate with the AMC partner and ensure resolution of all such issues.
11. The Bidder shall be responsible for configuring and providing the reports from the AD Server automatically through e-mails as required by OICL.
12. Design and Implement containers to segregate Laptops, Desktops and Servers.
13. The Bidder is expected to liaison with network / software and AMC partner of OICL to implement AD Services at all OICL offices.
14. The Bidder is expected to provide details regarding Active Directory network so as to give OICL sufficient insight on working of the software.
15. Bidder is required to provide the detailed architecture and design of the proposed Active Directory solution.
16. The proposed solution should support suitable business continuity and disaster recovery plan in the absence of availability of AD servers. The proposed solution should not hamper OICL's business at any case and at any time due to non-availability of AD servers.
17. The Active Directory logical structure should be in line with the organizational structure of OICL. Bidder is expected to configure active directory for group policies and security policies in concurrence with OICL.
18. Bidder will ensure that AD is able to implement policies on the bandwidth available during office hours without affecting the normal course of work. Bidder to note that during night hours and holidays, it will not possible to keep the desktops ON.
19. In case any problem (**bulk issues**) occurs in any of the authorized software/application of OICL due to the proposed solution, Bidder has to coordinate with OICL/ Application Vendor / AMC Vendor & resolve the



same during the tenure of the contract. However, field support will be done by respective AMC vendors of OICL.

20. Bidder shall submit procedural documents related to day-to-day operations, backup, restoration etc.
21. Bidder shall provide draft implementation plan along with the technical bid. Bidder will also have to document its post installation configuration and settings as part of the Post Installation System Configuration Document.
22. Bidder will be responsible for performing ongoing maintenance.
23. The Successful Bidder shall submit a detailed implementation strategy/ plan vetted by the OEM before and after implementation.
24. Bidder is required to factor in hours for Microsoft professional services as mentioned in the Bill of Material.

2.3.3 Antivirus Solution with EDR Functionality

OICL envisages to procure and implement the latest end point security solution for its 10,000 users

1. The bidder will be responsible for deploying the endpoint solution (including uninstallation of existing endpoint agent). Currently OICL is using Symantec end point security solution.
2. The solution should be deployed in a centralized architecture with management servers located at DC/DR. OICL will provide the required hardware along with Windows operating system for management, intermediary & updation of servers. Any other software like database etc. required for successfully running of the solution is to be factored by the bidder.
3. DR solution should be 100% of the DC Configuration.
4. The responsibility of Bidder is to maintain/manage/support which includes patches, updates and upgrades required for the successful implementation of AV across all OICL offices.
5. For OICL offices, Bidder is required to provide a mechanism to ensure regular updates of Antivirus Updates / patches / virus definitions on desktops and servers.
6. Bidder is required to ensure that the proposed AV should be able to install its agents and send updates / patches and receive status on the available bandwidth during office hours without affecting the normal work of the office. Bidder to note that during the night hours and holidays, it will not possible to keep the desktops ON.
7. The proposed AV solution should be able to update the definition files at the available bandwidth.
8. Solution must have an option to effectively utilize the bandwidth using bandwidth throttling mechanism during business hours and non-business hours.
9. Monthly reports giving information like updated antivirus clients, non-updated antivirus clients, version details and any other reports specified by OICL should be provided to Head Office/Regional Offices.
10. In case any problem (bulk issues) occurs in any of the authorized software/application of OICL due to the proposed solution, Bidder is required to coordinate with OICL/ Application Vendor / AMC Vendor of OICL & resolve the same during the tenure of contract.
11. If any issue arises, during AV Installation in Desktops, the Bidder's resources shall be responsible for coordinating with AMC partner and ensure resolution of all such issues. However, field support will be done by respective AMC vendors.
12. Bidder is required to provide OEM's highest level support for the entire contract duration.
13. Bidder shall also submit procedural documents related to day to day operations, backup, restoration.



14. Bidder to submit a draft implementation plan along with the technical bid. The Bidder will also have to document the post installation configuration and settings as part of the Post Installation System Configuration Document.
15. Successful Bidder shall submit the detailed implementation strategy/ plan vetted by OEM before and after implementation.
16. For being committed to the success of the project and take ownership during the actual implementation, it is the responsibility of the bidder to ensure involvement of OEM for various aspects of project including sizing, requirement gathering, configuration, customization, performance tuning, implementation support, setting up of production environment. The Bidder shall provision for requisite support as part of Appendix 2- Commercial Bill of Material. OEM's involvement for implementation of Antivirus with EDR should be minimum 10% of the overall implementation effort being proposed by the bidder during the implementation.

The solution should meet all the requirements as per the technical specifications given in this RFP.

2.3.4 Enterprise Management System

The Bidder shall supply, install, configure and maintain the Enterprise Management System to meet the scope. OICL will provide the servers. Bidder is required to submit the sizing and factor in for any database or other hardware reqd. for successful commissioning.

1. The responsibility of the Bidder is to maintain/manage/support the proposed solution which includes patches, updates, upgrades and implementation of EMS.
2. The Bidder is required to document the post installation configurations and settings as part a Post Installation System Configuration Document. Bidder should provide a draft plan of the same along with the technical bid.
3. DR solution should be 100% of the DC Configuration.
4. Bidder to ensure that the solution is working in line with the industry leading practices and is compliant with ITIL standards.
5. Bidder shall carry out the asset management of all networked devices across all OICL offices. It shall also support auto-discovery of equipment and should be able generate online reports without any manual intervention.
6. Integrated reporting should be fully automatic with no manual intervention. All modules of EMS should be integrated with the Helpdesk solution.
7. Bidder to ensure that EMS is able to install its agents and send updates / patches and receive status on the bandwidth available during office hours without affecting the normal work of the office. Bidder to note that during night hours and holidays, it will not possible to keep the desktops ON.
8. The proposed solution should be synced with Active Directory.
9. Solution should have an option to effectively utilize the bandwidth using bandwidth throttling mechanism during business hours and non-business hours.
10. Bidder is required to provide a console of EMS solution at HO and 30 Regions for their respective regions with view right only.
11. Removal of unauthorized software with confirmation from OICL.



12. For EMS Installation in Desktops, if any issue arises, Bidder's resource shall be responsible for coordination with AMC partner and ensure resolution of all such issues. However, Field support will be done by respective AMC vendors.
13. Bidder to ensure that OS monthly patches are sent centrally through EMS.
14. Bidder to ensure that the proposed EMS is able to detect the older versions of the installed authorized software and update it.
15. Bidder to ensure that the proposed EMS is capable of detecting unauthorized software(s) installed in endpoints and delete the same.
16. Bidder to submit procedural documents related to day-to-day operations, backup, restoration.
17. Bidder to provide a draft implementation plan along with the technical bid. The Bidder will also have to document the Post installation configuration and settings as part of the Post Installation System Configuration Document.
18. The successful bidder should submit the detailed implementation strategy/ plan vetted by OEM before and after implementation.
19. For being committed to the success of the project and take ownership during the actual implementation, it is the responsibility of the bidder to ensure involvement of OEM for various aspects of project including sizing, requirement gathering, configuration, customization, performance tuning, implementation support, setting up of production environment. The Bidder shall provision for requisite support as part of Appendix 2- Commercial Bill of Material. OEM's involvement for implementation of EMS should be minimum 10% of the overall implementation effort being proposed by the bidder during the implementation.

Bidder should comply with the specifications & modules as mentioned in Appendix 1.

2.3.5 Helpdesk Solution

Bidder is expected to supply, implement, commission, and maintain the helpdesk. The helpdesk should act as a single point of contact for all users whether for service requests, incidents or problems. It should encompass Helpdesk, EMS, AD & AV (including EDR) issues. In addition, it should offer a focussed approach for delivering integrated service management. It should provide an interface for other functions in IT Services Continuity Management like maintenance contracts, software licenses, Service Level Management, and Financial Management.

OICL has its head office at New Delhi and 30 Regional Offices across the country.

1. The Bidder is required to establish and maintain a Help Desk Solution as a Single Point of Contact for all services, solutions & infrastructure at OICL, for lodging complaints with their respective AMC vendors, generating ticket numbers, tracking complaints, routing service requests until closure of call.
2. The Bidder is required to extend the helpdesk solution to all users under the Head Office at New Delhi and all 30 Regional Offices by providing interface/logins for lodging complaints with their respective AMC Vendors.
3. Bidder is required to customize the Helpdesk Solution for HO and all 30 RO's by implementing their SLA terms with their respective AMC Vendors in the helpdesk portal.
4. Bidder is required to provide a dashboard console as well as a reporting mechanism to HO and all 30 RO's for analyzing the complaints. In addition, the Bidder has to provide a mechanism to Head Office to centrally monitor & report the performance of Regional Offices, if required.



5. OICL requires a separate help-desk partition which shall be common for HO and all 30 RO's with common SLA and access rights to all users under HO and RO's.
6. Access to the Helpdesk solution must be provided to HO and all 30 RO's. One for Regional IT Coordinator for monitoring the complaints under their Region and for penalty calculation and one admin login for the AMC partner of each of the locations, for updating the status of the complaints lodged under their region and for managing the SLA terms and conditions.
7. Helpdesk solution should have the capability to upload frequently asked questions.
8. It should incorporate an individual escalation matrix of HO and all 30 RO's and should have a provision to escalate issues pertaining to user's non-availability or non-cooperation of the vendor.
9. Generate service management reports from the ticketing tool.
10. Maintenance of an SLA matrix.
11. Notifying users of problem status and resolution (via mails).
12. Tracking of problems from an initial call to restore to service. This includes problems redirected to nonBidder service providers
13. Monitoring systems to proactively determine, diagnose, and resolve problems. This includes notifying customers and all service providers of known problems and alerts;
14. Provide reports that effectively summarize and communicate the performance and compliance with service levels defined in OICL's service level agreement (SLA) with the Vendor. OICL will have the ability to directly generate standard and ad hoc reports as needed from the same helpdesk setup;
15. Proposed solution shall be customizable as per requirements of OICL.
16. Bidder has to maintain the backup of logged calls of individual Regional Office's during the contract period & shall provide the same to OICL as and when required. (On a Daily/Weekly/Monthly basis)
17. Bidder shall provide separate partitions of help desk solution to handle SLA's of other OICL business applications like HRMS, Web Portal Application, and new upcoming applications during the contract period.
18. Bidder shall provide an efficient and prompt solution to operational problems of end users concerning the application system. Bidder shall implement effective helpdesk management procedures to leverage the knowledge gained in providing faster and better solutions, create knowledge bases and prevent recurrence of problems.
19. Successful Bidder shall submit the detailed implementation strategy/ plan vetted by OEM before and after implementation.
20. For being committed to the success of the project and take ownership during the actual implementation, it is the responsibility of the bidder to ensure involvement of OEM for various aspects of project including sizing, requirement gathering, configuration, customization, performance tuning, implementation support, setting up of production environment. The Bidder shall provision for requisite support as part of Appendix 2- Commercial Bill of Material. OEM's involvement for implementation of Helpdesk solution should be minimum 10% of the overall implementation effort being proposed by the bidder during the implementation.

Bidder should comply with the specifications as mentioned in Appendix 1

2.3.6 OEM's Scope

For being committed to the success of the project and take ownership during the actual implementation, it is the responsibility of the bidder to ensure involvement of OEM for various aspects of project including sizing,



requirement gathering, configuration, customization, performance tuning, implementation support, setting up of production environment for AV+EDR, EMS & Helpdesk Solution. The Bidder shall provision for requisite support as part of Appendix 2- Commercial Bill of Material. OEM's involvement for implementation of AV+EDR, EMS & Helpdesk solution should be minimum 10% of the overall implementation effort being proposed by the bidder during the implementation. Below mentioned activities are to mandatorily be carried out by the OEM.

S.No.	Deliverable	Application OEM Responsibility
1	Project Plan	OEM to review the Project plan submitted by the Bidder
2	SRS Document	OEM to validate the SRS document submitted by the Bidder
3	HLD/ LLD	Bidder to take inputs from the OEM and provide LLD & HLD documents to OICL. However, it is the responsibility of the OEM to review and recommend a methodology to achieve best performance. The same needs to be implemented upon sign-off on the documents by OICL.
4	Data Migration Strategy	OEM to validate the Data Migration Approach prepared by the Bidder which should broadly include the approach for data held in existing application, template formats in which data is required from legacy systems, execution of migration utilities on the data and resolving the issue for any inconsistency in the data etc.
5	SIT & UAT	OEM to assist in SIT and UAT
6	Base Product Patches	OEM to provide all patches related to Product, Customizations and Interfaces within the agreed timelines.
S.No.	Deliverable	Application OEM Responsibility
		OEM to reconcile the product and other patches provided to OICL in a manner that the same is available on Day 1 to OICL.
7	Go-Live	OEM to assist in having hygiene factors in place for checks and closures of SIT/ UAT/ correctness of data. OEM should be available during the Go-live period to address any bugs raised during the go-live phase.
8	Status Reports	OEM till implementation closure is required to be a part of the status calls from an application point of view to provide timelines for bug closures. The OEM Involvement is required during the project review meeting throughout the implementation period
9	Documentation	OEM to share the following: <ul style="list-style-type: none">✓ Product manuals✓ Technical manuals✓ Data Dictionary of the Product

2.3.7 Facilities Management (FM) & Annual Technical Support (ATS)

The successful Bidder should depute qualified dedicated manpower (FM support Engineers) from the date of project sign off till the contract expiry date at OICL Head Office, New Delhi as per OICL's office hours.



Bidder will be the single point of contact and responsible for ATS, guarantees & warranties for all components, software, etc. While bidding for providing facilities management services, the products and solutions proposed by the Bidder by way of this RFP should come with warranty as provided by the respective OEMs. Thereafter, the Bidder should provide ATS/ AMC for these products and solutions **(after the warranty of 3 Years for Software)**.

Warranties pertaining to Software / Applications starts post deployment of licenses in the production. The period of warranty is three years. ATS for Software/ Application shall begin post Completion of Warranty.

All proposed resources are required to have the following minimum qualification:

Project Manager

The proposed resources should have 5-7 years of experience

Active Directory

The proposed resources should be a Microsoft Certified Engineer having expertise in Domain Policies with Minimum 3 Years of Experience in handling Active Directory Solution.

Anti-Virus

The proposed resources should be certified in the proposed solution with Minimum 3 Years of Experience in handling proposed/ similar AV Solution.

EDR

The proposed resource should be certified in the proposed solution with Minimum 1 Year of Experience in handling proposed/ similar EDR Solution.

Enterprise Management System

The proposed resources should be certified in the proposed solution with Minimum 3 Years of Experience in handling proposed/ similar EMS.

Helpdesk Coordinator

The proposed resources should at least be a graduate/diploma holder in engineering (IT/Electronics/Computers) having good knowledge in similar solution.

1. FM engineer(s) should be trained & experienced professionals having excellent communication skills. The FM resources should be minimum graduate/diploma holder in engineering (IT/Electronics/Computers) or B.Sc (IT/CS)/ BCA having good knowledge on Directory Services, Enterprise Management Software & Anti-Virus (AV) Solution. The FM resource(s) should have a Certification in the Proposed Directory Services / Enterprise Management software/ AV solution.
2. In case the engineer goes on leave / absent, OICL should be intimated prior to taking leave and suitable replacements/backup should be arranged by the Bidder to ensure that regular functioning of the offices do not get hampered. The bidder has to provide the resumes of new resources. These new resources should have the same specialization as mentioned above.
3. The proposed resources can be transferred to OICL's Data Center Sites, if required.
4. If required, resources will be required to travel as and when required to OICL's DC / DRC locations at bidders own cost.



5. In case OICL intends either to replace the existing old Desktops with the new Desktops (transition phase), or there is an increase in the count of Desktops during the contract period there shall be no change in the commercial value of the FMS resources.
6. FMS Resources shall be responsible for system configuration of Servers at DC & DR Site. Also, FM Resources will have to ensure the update of latest patches & Operating System along with required security settings, network settings, etc. to run the proposed solution error-free.
7. All updates of the proposed solution for the application software and endpoints have to be done after proper testing. Confirmation of testing shall be the responsibility of the bidder.
8. FM Resources shall also be responsible for maintenance of the FTP Server provided by OICL.
9. FMS Resources shall coordinate with the AMC Vendor of all regions and provide confirmation for installation & commissioning of the procured solution(s) to maintain the compliance level of proposed solution.
10. FM Resources shall be responsible to maintain the inventory list of the assets. However, entry & tagging shall be done by respective Regions.
11. OICL will provide the necessary seating space, furnishing, and electrical connections for the same. Bidder has to provide Desktops, PSTN telephones with STD facility, Toll Free Number etc. for the proposed resources.
12. The Bidder has to provide the telephonic, electronic mechanisms and software based tool for reporting problems of AD/AV/EMS, issue a ticket number for all calls entered, acknowledge the tickets, allocate appropriate category requests for service, update status and resolve the issues. Bidder has to maintain the backup of logged calls during the contract period & shall provide the same as per OICL's requirement (Daily/Weekly/Monthly basis).
13. FM shall coordinate for the following list of activities:
 - a. Providing a Single Point of Contact (SPOC) for assistance with IT services under scope. It should encompass Helpdesk, EMS, AD & AV (including EDR) issues. In addition, it should offer a focused approach for delivering integrated Service Management.
 - b. One time and Regular Documentation of installation/ implementation/maintenance procedure for AD/AV/EMS software for end point systems at Operation Offices as and when required by OICL.
 - c. In case of any problem regarding AD/AV/EMS software at operating offices, NOC Team will coordinate with HO/RO administrators and respective AMC partners to troubleshoot the problem and will prepare the documentation for the same.
 - d. Sending reports of Anti-virus, Enterprise Management Solution, and Active Directory etc. to HO and ROs as per OICL's requirements.
 - e. FM Resource should provide details related to new OS patches/ hot-fixes released in Desktops & Servers. FMS Resource shall also be responsible for update / upgrade of these patches/hot-fixes.
 - f. In case bidder requires to configure the local servers of the proposed solution at OICL offices for smooth and timely updates of endpoints along with implementation of the policies, bidder shall only be responsible to manage the same, however, if any field support is required, OICL shall provide the same.



- g. FM resources shall also be responsible for coordinating with the AMC partners of respective regions of OICL, for installation and commissioning of proposed solution when escalated through HO IT.
- h. Generate service management reports from the ticketing tool.
- i. Maintenance of SLA matrix.

2.3.8 Project Management

Bidder is required to deploy a project manager at OICL's head office who will be responsible for managing the project as a whole and act as an interface between OICL and the Bidder during the contract period. Project Manager will be the single point of contact on behalf of the Bidder.

Bidder should provide a detailed description for project management activities as part of its proposal in response and compliance to this RFP.

Project Manager Responsibilities would primarily cover the following:

- a. To ensure service 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 design, implement and demonstrate processes in line with best practices.
- e. To factor resource redundancy plan for better continuity and reliability of services.
- f. To create documentation for all the processes in line with quality standards.
- g. Ensuring continuous improvement of services
- h. Sharing knowledge and value addition with OICL's IT team on continuous basis.
- i. Innovative and effective use of EMS tools in delivering services
- j. Overall responsibility for delivery of services as per Scope/ Statement of Work/s (SOW) and Service Level Agreement (SLA).
- k. Maintain project communications with stakeholders of OICL
- l. Provide strategic and tactical recommendations in relation to technology related issues and technology improvement.
- m. Resolve deviations from the phased project plan.
- n. Conduct regular scheduled project status/ review meetings involving officials of the Bidder and OICL
- o. Submission of periodic reports

2.3.9 Transition Management

OICL recognizes that the transition process and its effectiveness, has a significant impact on the success of the ongoing services. OICL has the following key objectives for transition:

- a) Maintain steady operation of all services and maintenance of current service levels during migration of controls and responsibility from OICL / current vendor to selected Bidder.
- b) Successfully complete all activities, providing a stable platform for future improvement in service delivery and associated benefits for OICL Transition Deliverables.



2.3.10 Training

The Bidder shall provide OICL with a comprehensive training program that includes instructor-led training to facilitate successful implementation and knowledge transfer of the proposed solution.

Training schedule is defined in Appendix 2: Bill of Material

****Each batch should accommodate additional 20% of resources over and above the limit prescribed**

- At the end of each training session, an evaluation test needs to be conducted to ascertain the effectiveness of the training.
- Training deliverables shall be
 - User Training Plan
 - Training Material (in English)
 - User Manuals including customizations specifically done for OICL.

2.3.11 Documentation

The Bidder shall provide the following documents along with the technical bid:

1. The Bidder will have to develop a detailed system design document for all the services in consultation with OICL. Provide a template for system design document along with the technical bid.
2. The Bidder is also required to develop and document detailed system administration and maintenance procedures customized for OICL. These documents will serve as a guide for OICL administrators while managing the project.
3. System Design Document should be OEM vetted.
4. System Design Document should be updated once each quarter.
5. Part coded technical Bill of Material.
6. Datasheets of the proposed products.

2.3.12 Reporting

Bidder is required to submit the reports on a regular basis in a mutually decided format. The following is an indicative list of reports that would be required to be configured for AD, AV (including EDR), EMS & Helpdesk. Softcopy of these reports shall be delivered automatically/manually via email at mutually decided frequency and to the pre-decided list of recipients.

Role based selection of reports, selection of name of the recipients of the reports; frequency of delivery must be parameterized/ configurable by FM team.

Bidder shall submit certain information as part of periodic review as and when required by OICL.

The following is the indicative list of reports:

1. Daily Reports (to be submitted daily)

- a) Daily Reports of AD, AV with EDR, EMS.
- b) Summary of issues / complaints logged at the Help Desk.
- c) Summary of resolved, unresolved and escalated issues / complaints.
- d) Summary of resolved, unresolved and escalated issues / complaints to OEMs/ vendors/OICL support teams.
- e) Availability and Resource Utilization



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

- a) Issues / Complaints Analysis report for virus calls, call trend, call history etc.
- b) Summary of systems (server) rebooted.
- c) Summary of issues / complaints logged with the OEMs.
- d) Availability and Resource Utilization
- e) Inventory Reports.

3. Monthly reports (to be submitted by 10th of the following month)

- a) Availability and Resource Utilization
- b) Summary of changes in the Data Centre.
- c) Service Level Management – priority/ severity wise response and resolution.
- d) Service Failure Analysis, listing out escalations and downtime/ outages, if any.
- e) Service Operations, listing out:
 - i. Service Desk Management – Location wise call summary for all on-site FM locations for last three months.
 - ii. Helpdesk Management, listing out priority/ severity wise calls logged with comparison for past three months.
- f) Service Improvement Plan, listing out:
 - i. Concerns/ Escalations with action plan.
 - ii. Planned activities/ initiatives.
 - iii. Improvements planned, if any.

4. Incident Reporting (to be submitted within 48 hours of the incident)

- a) Detection of security vulnerability with the available solutions / workarounds for fixing.
- b) Hacker attacks, Virus attacks, unauthorized access, security threats, etc. with root cause analysis and plan to fix the problems.
- c) Software license violations.

Reporting also includes any report as per observations during audit or as per OICL's requirements.

2.3.13 Escrow

OICL and the Bidder shall agree to appoint an escrow agent to provide escrow mechanism for the deposit of the source code of any customization done on Commercial off the shelf software products supplied/ procured by the Bidder to OICL for EMS & Helpdesk Solution in order to protect its interests in an eventual situation. OICL and the selected bidder shall enter into a tripartite escrow agreement with the designated escrow agent, which will set out, inter alia, the events of the release of the source code and the obligations of the escrow agent. Costs for the Escrow will be borne by the Vendor

2.4 Geographical Location

For the purpose of solution/equipment implementation, the location of different sites is as follows:

Site Name	City	State
Primary Data Centre (DC)	Bengaluru	Karnataka
Secondary Data Center (DR)	Navi Mumbai	Maharashtra

Note: If OICL shifts any of the sites to a new location, the successful Bidder shall provide respective services from the new location.



3 Terms & Conditions

3.1 General

3.1.1 Definitions

OICL/ PURCHASER/ BUYER: Shall mean The Oriental Insurance Company Limited

3.1.2 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 <https://orientalinsurance.org.in>.

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.

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.

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

Bidder shall have the opportunity to clarify doubts pertaining to the RFP in order to clarify any issues they may have, prior to finalizing their responses. All queries/questions are to be submitted to the Deputy General Manager, IT at the address mentioned below and should be received by the point of contact not later than the date and time specified in section 1.4 Schedule of Events. Responses to inquiries and any other corrections and amendments will be distributed to the Bidder by electronic mail format or hardcopy letter, at the sole discretion of OICL.

The Deputy General Manager
The Oriental Insurance Company Limited
Information Technology Department,
NBCC Office Complex, East Kidwai Nagar,
2nd Floor, Office Block 4,
New Delhi- 110023

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 OICL's decision in the matter will be final.



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.

OICL reserves the right to make any changes in the terms and conditions of purchase in accordance with the pre bid clarification. OICL will not be obliged to meet and have discussions with any Bidder, and / or to listen to any representations to changes made after pre-bid clarification.

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.

Right to Alter Quantities – OICL reserves the right to alter the requirements specified in the tender. OICL also reserves the right to decrease or increase one or more items from the list of items specified in the tender subject to a maximum of +/-25%. 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.

3.1.3 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 subcontractors 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.

3.1.4 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.

3.1.5 Submission of Bids

Bidders shall submit the Bids online. For details, please refer RFP Section 6 – Instruction to Bidders.

3.1.6 Performance Security

Within 15 days after the receipt of Notification of Award from OICL, the Bidder shall furnish performance security to OICL as per Annexure - 6, which shall be equal to 3 percent (3%) of the value of the contract - valid till date of expiry of 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).

3.1.7 Pre-Bid Meeting

All queries/ requests for clarification from Bidders must reach us by e-mail



(tender@orientalinsurance.co.in) or in person. Format for the queries / clarification is provided in “Annexure 4 - 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.

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.

3.1.8 Delay in Bidder's performance

The start date for services 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.

3.1.9 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.

All / any payments will be made subject to compliance of Service Levels defined in the RFP document. 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. If any of the items / activities as mentioned in the price bid is not taken up by OICL during the course of the assignment, OICL will not pay the fees quoted by the Bidder in the price bid against such activity / item.

Payment terms are as follows:

#	Items	Milestone	Percentage
1	Software	Delivery of respective software & its related components as per the actual supply (after due inspection)	70%



#	Items	Milestone	Percentage
		Successful completion of customization and successful acceptance of software by OICL (after due inspection)	30%
2	Installation & Implementation Cost	On Successful go-live/ installation of solution/ product	100%
3	ATS/ AMC	The ATS/ AMC shall commence on completion of the warranty period. The ATS/ AMC will be treated as a part of the total cost of the project.	Annually in advance
4	FM Manpower		Quarterly in arrears
5	Training		100% after the completion
6	Escrow		Annually in Advance
7	Other Costs		In arrears post Completion of respective services

3.1.10 Mode of Payment

OICL shall make all payments only through Electronic Payment mechanism (viz. ECS).

3.1.11 Penalties and delays in Bidder's performance

In case the vendor fails to meet the SLA mentioned in section 8, penalty will be imposed as mentioned in section 7 Service Level Agreement

3.1.12 Currency of Payments

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

3.2 Other RFP Requirements

- The Head Office of OICL is floating this RFP. However, the Bidder getting the contract shall provide services, procured through this RFP, at OICL's DC and DRS or at such centers as OICL may deem fit and the changes, if any, in the locations will be intimated to the Bidder.
- Technical Inspection and Performance Evaluation - OICL may choose to carry out a technical inspection/audit and performance evaluation of products/services offered by the Bidder. The Bidder would permit OICL, or any person / persons appointed by OICL to observe the technical and performance evaluation / benchmarks carried out by the Bidder. Any expenses (performing the benchmark, travel, stay, etc.) incurred for the same would be borne by the Bidder and under no circumstances the same would be reimbursed to the Bidder by OICL.
- The Bidder's representative/local office at New Delhi will be the contact point for OICL. The delivery status of equipment/part should be reported on a weekly basis.



- d. OEM's Authorization Form – The Bidder should furnish a letter from original equipment manufacturer.

4 Terms of Reference ('ToR')

4.1 Contract Commitment

OICL intends that the contract, which is contemplated herein with the Bidder, shall be for a period of 6 years and extendable for one years on same Terms & Conditions and mutually agreed prices (solely at OICL's discretion).

4.2 Completeness of Project

The project will be deemed as incomplete if the desired objectives of the project Section 2 – Scope of Work of this document are not achieved and the decision of OICL shall be final.

4.3 Compliance

Compliance with all applicable laws: The Bidder shall undertake to observe, adhere to, abide by, comply with and notify OICL about all laws in force including labor laws or as are or as made applicable in future, pertaining to or applicable to them, their business, their employees or their obligations towards them and all purposes of this tender and shall indemnify, keep indemnified, hold harmless, defend and protect OICL and its employees/officers/ staff/ personnel/ representatives/agents from any failure or omission on its part to do so and against all claims or demands of liability and all consequences that may occur or arise for any default or failure on its part to conform or comply with the above and all other statutory obligations arising there from.

Compliance in obtaining approvals/permissions/licenses: The Bidder shall promptly and timely obtain all such consents, permissions, approvals, licenses, etc., as may be necessary or required for any of the purposes of this project or for the conduct of their own business under any applicable Law, Government Regulation/Guidelines and shall keep the same valid and in force during the term of the project, and in the event of any failure or omission to do so, shall indemnify, keep indemnified, hold harmless, defend, protect and fully compensate OICL and its employees/ officers/ staff/ personnel/ representatives/ agents from and against all claims or demands of liability and all consequences that may occur or arise for any default or failure on its part to conform or comply with the above and all other statutory obligations arising there from and OICL will give notice of any such claim or demand of liability within reasonable time to the Bidder.

This indemnification is only a remedy for OICL. The Bidder is not absolved from its responsibility of complying with the statutory obligations as specified above. Indemnity would be limited to court awarded damages and shall exclude indirect, consequential and incidental damages. However, indemnity would cover damages, loss or liabilities suffered by OICL arising out of claims made by its customers and/or regulatory authorities.

4.4 Assignment

OICL may assign the Services 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 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 favorable 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.

4.5 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.

4.6 Indemnity

The Bidder 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
- d) Indemnity would be limited to court awarded damages and shall exclude indirect, consequential and incidental damages.

4.7 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.

4.8 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.

4.9 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.



4.10 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.

4.11 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.

4.12 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 as on the date of bid submission

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 with equivalent or higher capacity hardware/software at no additional cost to OICL.

4.13 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 ensure 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 loss, 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.

4.14 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, pandemic, 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.

4.15 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, Tools 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.

4.16 Liquidated Damages

If the Bidder fails to meet the Project Timelines 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 total contract price. Once the maximum is reached, OICL may consider termination of the contract.

4.17 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.

4.18 Termination for Convenience

OICL may send by 30 calendar days written notice to the Bidder to 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. In the event of the Bidder wishing to terminate this agreement, the Bidder may send by 90 calendar days written notice to OICL to 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 and the decision of OICL shall be final.

4.19 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.

4.20 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.

4.21 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)

4.22 Prices

The prices quoted (as mentioned in Appendix 2 – Commercial Bill of Material 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.

4.23 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, 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.

4.24 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.

4.25 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 favor of OICL in such forms as shall be required by OICL after all payments due to the Bidder/Supplier are made in full.

4.26 Cancellation of the contract & compensation

OICL reserves the right to cancel the contract placed on the selected Bidder and recover expenditure incurred by the Company in the following circumstances:

- i. The selected Bidder commits a breach of any of the terms and conditions of the bid.
- ii. The selected Bidder goes in to liquidation voluntarily or otherwise.
- iii. The progress made by the selected Bidder is found to be unsatisfactory
- iv. If deductions on account of liquidated Damages exceeds more than 10% of the total contract price.



OICL reserves the right to cancel the AMC placed on the selected Bidder and recover AMC payment made by the Company, if the service provided by them is not satisfactory.

In case the selected Bidder fails to deliver the quantity as stipulated in the delivery schedule, OICL reserves the right to procure the same or similar materials from alternate sources at the risk, cost and responsibility (capped at 5% differential value) of the selected Bidder. After the award of the contract, if the selected Bidder does not perform satisfactorily or delays execution of the contract, OICL reserves the right to get the balance contract executed by another party of its choice by giving thirty day's written notice for the same to Bidder. In this event, the selected Bidder is bound to make good the additional expenditure (capped at 5% differential value), which OICL may have to incur in executing the balance of the contract. This clause is applicable, if for any reason, the contract is cancelled.

If the Contract is cancelled during AMC, OICL shall deduct payment on pro-rata basis for the unexpired period of the contract

4.27 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.

4.28 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.

4.29 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.

4.30 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.



4.31 Adherence to Terms and Conditions

The Bidders who wish to submit responses to this RFP shall abide by all the terms and conditions contained in the RFP. If the responses contain any extraneous conditions put in by the Bidder, such responses may be disqualified and may not be considered for the selection process.

4.32 Integrity Pact

To ensure transparency, equity, and competitiveness and in compliance with the CVC guidelines, this tender shall be covered under the Integrity Pact (IP) policy of OICL. The pact essentially envisages an agreement between the prospective bidders/vendors and OICL committing the persons/officials of both the parties, not to exercise any corrupt influence on any aspect of the contract. The format of the agreement is enclosed in Annexure 12.

Signing of the IP with OICL would be one of the preliminary qualification for further evaluation. In other words, entering into this pact would be one of the preliminary qualification for this tender and the pact shall be effective from the stage of invitation of bids till the complete execution of the contract. Any vendor/bidder not signed the document or refusing to sign shall be disqualified in the bidding process.

The Integrity Pact envisages a panel of Independent External Monitors (IEMs) to review independently and objectively, whether and to what extent parties have complied with their obligation under the pact. The IEM has the right to access to all the project document. **Capt. ANOOP KUMAR SHARMA** and **Shri H.K DASH, IAS (Retd.)** shall be acting as the IEM for this contract/Tender. However, OICL at its sole discretion reserves the right to change/name another IEM, which shall be notified latter.

Contact Details:

Capt. ANOOP KUMAR SHARMA	SHRI H.K.DASH, IAS (Retd.)
2104 A, Oberoi Gardens, Thakur Village, Kandivili (East), Mumbai-400 1 Mobile No: 8291086676 Email ID: anoop21860@gmail.com	House no. 289, Sector-8 Gandhinagar- 382007 Gujarat Mobile: 98250-48286 Email ID: hkdash184@hotmail.com

4.33 Outsourcing Agreement

The outsourcing contract, inter alia, shall have in place following clauses or conditions listed below: -

- 1. Contingency Planning:** The Bidder is responsible for contingency planning of the outsourcing service to provide business continuity for the outsourced arrangements that are material in nature.
- 2. Express Clause:** The contract shall neither prevent nor impede the company from meeting its respective regulatory obligations, nor the IRDAI from exercising its regulatory powers of conducting inspection, investigation, obtaining information from either the company or the Bidder.
- 3. Handing over of the Data, Assets etc.:** In case of termination of the contract, the Bidder is responsible for handing over of the data, assets (hardware/software) or any other relevant information specific to the contract and ensure that there is no further use of the same by the Bidder.
- 4. Inspection and Audit by the Company:** The Company shall conduct periodic inspection or audit on the Bidder either by internal auditors or by Chartered Accountant firms appointed by the Company to examine the compliance of the outsourcing agreement while carrying out the activities outsourced.



- 5. Legal and Regulatory Obligations:** The Bidder shall ensure that the outsourcing contract/ arrangements do not: -
- a) Diminish the Company's ability to fulfil their obligations to Policyholders and the IRDAI.
 - b) Impede effective supervision by the IRDAI.
 - c) Result in Company's internal control, business conduct or reputation being compromised or weakened.
- 6. Applicability of the laws/regulations:** The Regulations apply irrespective of whether the outsourcing arrangements are entered into with an affiliated entity within the same group as the Company, or an outsourcing service Provider external to the group or the one who has been given sub-contract. The Outsourcing Agreement shall not diminish the obligations of the Company and its Board & Senior Management to comply with the relevant law/s and regulations. The Bidder engaged by the company is subject to the provisions of the Insurance Act 1938, IRDA Act 1999, rules & regulations and any other order issued thereunder.

In case, the Bidder operates from outside India, it shall ensure that the terms of the agreement are in compliance with respective local regulations governing the Bidder and laws of the country concerned and such laws and regulations do not impede the regulatory access and oversight by the Authority.

4.34 Regulations, Legal & Compliance

Communications made via OICL's Social Media channels will in no way constitute a legal or official notice to OICL or any official or employee of OICL for any purpose.

Any content that the Bidder posts on OICL's Social Media channels shall be deemed and remain the property of OICL. OICL shall be free to use such content/ information, for any purpose without any legal or financial compensation or permission for such usage.

OICL reserves its rights to initiate appropriate legal proceedings in the event of any breach/ violation of these guidelines/ other terms and conditions as may be specified by OICL from time to time.

Under no circumstances OICL shall or any of our affiliates, employees or representatives, be liable to the Bidder for any direct or indirect, claims or damages whatsoever emanating from any mistakes, inaccuracies, or errors of content, personal injury or property damage, of any nature whatsoever, emanating from your use to and access of our Social Media platforms or entities purporting to represent OICL. Bidder specifically acknowledge that OICL shall not take any liability for content or the offensive, defamatory, or illegal conduct of any third party and that the risk of damage or harm arising from the preceding entirely rests with the bidder. The foregoing limitation of liability shall apply to the fullest extent that's permitted by law in the applicable jurisdiction.

To the extent permitted by law applicable, bidder agree to indemnify, defend and hold harmless, OICL, its affiliates, officers, directors, employees, and agents, arising from and against any and all damages, claims, obligations, liabilities, losses, costs or debt, and expenses (including but not limited to lawyer's/attorney's fees) arising from: (i) use of and access of our page; (ii) violation of any of these Guidelines; (iii) violation of any third party right, including without limitation any copyright, proprietary, or right to privacy; or (iv) all or any claim that content posted by you caused damage to a third party. The indemnification obligation contained herein shall survive these Guidelines and your use of our Social Media channels.



Anyone causes or knowing that he/ she is likely to cause wrongful loss or damage to the brand's image, to destroy or delete or alter any information residing on the Social Media platform or diminish its value or utility by any means, commits hack, shall be prosecuted under Information Technology Act, 2000 [As amended by Information Technology (Amendment) Act 2008], its subsequent amendments as well as any other statute prescribed by the concerned authorities.

4.35 Guidelines for MSME

As per the public Procurement Policy for MSEs order, 2018 under section 11 of MSMED Act 2006 MSEs quoting price within band L-1 +15% when L1 is from someone other than MSE, shall be allowed to supply at least 25% of tendered value at L-1 subject to lowering of price by MSEs to L-1.

However, seeing the criticality, stack sync and manageability of the devices which are the core element to provide services to the customer the entire order will go to one vendor in the above-mentioned case.

4.36 Transfer of Title

Title of ownership of goods supplied under this contract passed on to OICL on delivery of goods at the site.

5 Instruction to Bidders

5.1 Instructions for Online Bid Submission

- Bidders should comply to rules and regulations of GeM portal for submission of Bids online.
However, Bidder needs to submit the commercial bill of material i.e., Appendix 2: Bill of Material, Annexure 11:- NDA, Annexure 12 – Integrity Pact and Power of Attorney on stamp Paper in offline mode to OICL Head office in a sealed envelope.
- The sealed envelope should be properly labeled with the company name, RFP number, date and duly signed and stamped. If Bidder did not submit the same, then Bidder will be disqualified.
- The Sealed envelope should reach OICL before or on the date and time of submission schedule as mentioned in the RFP.
- Bidder needs to fill the bill of material properly and the total value in bill of material should match with the total value mentioned in the GEM Portal.
- If there is any mismatch between the total value of the Sealed envelope and the GEM portal, then the bid of the Bidder will be rejected.
- OICL will not be liable of the any arithmetic error in the bill of material, and the GEM final number will be accepted as the Total cost of the Project.
- If Bidder misses or forgets to quote rates of any line item, then it is assumed that Bidder will provide that service at zero cost to OICL during contact period.

5.2 Tender Bidding Methodology

Sealed Bid System.

The Bidders will be required to submit following two sets of separate documents.

- Eligibility & Technical Bid



2. Commercial Bid

5.3 Bid Security

Govt. of India guideline vide Circular dated F.9/4/2020- PPD dated 12th November 2020, states:

“It is reiterated that notwithstanding anything contained in Rule 171 of GFRs 2017 or any other Rule or any provision contained in the Procurement Manuals, no provisions regarding Bid Security should be kept in the Bid Documents in future and only provision for Bid Security Declaration should be kept in the Bid Documents.”

Hence, in conformance to the above, Bidders are to submit Bid Security Declaration as per format provided in Annexure 5.

6 Bid Documents

6.1 Eligibility Bid Documents

1. Compliance to Eligibility Criteria as per RFP Section 1.6 along with all relevant supporting documents
2. Application Form for Eligibility Bid as per Annexure 1
3. The references of Bidder's clients. Also provide the name, designation, and contact details of a contact person for each reference as per Annexure 2.
4. The corporate profile of the Bidder (printed corporate brochure is preferred).
5. The profile of the Bidder (as per Annexure 9)
6. List of Bidder's support/service locations in India as per Annexure 8.
7. Bidder shall submit PAN number, GSTIN.
8. Undertaking that the Bidder has quoted for all items and the bid validity will be for 180 days from the date of submission of bid.
9. The power of attorney or authorization, or any other document consisting of adequate proof of the ability of the signatory to bind the Bidder
10. Statement of No-Deviation (Annexure 7)
11. Integrity Pact (Annexure 12 on Stamp Paper)
12. Bid Security Declaration as per Annexure 5
13. NDA as per Annexure 11 on stamp paper
14. MAF as per Annexure 14

6.2 Technical Bid Documents

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. The Executive Summary should initially provide an overview of Bidder's organization and position with regards to proposed solution and professional services. A summary of the Bidder's products and services that will be provided as a part of this procurement should follow.
2. Detailed technical note covering the detailed scope of work.
3. Compliance to Technical Specifications as per Appendix 1.
4. The Bidder should also include a replica of the masked 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 2 – Bill of Material in the RFP.

5. Part coded Technical Bill of Material
6. Implementation plan & warranty support
7. Support Plan
8. User Training Plan
9. Transition Plan
10. Escalation matrix
11. Undertaking from Bidder for providing authorized representatives of IRDAI the right to inspection, investigation, obtaining information (Annexure 10).

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.
4. 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.
5. 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.
6. 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.

6.3 Commercial Bid Documents

Commercial Bid should contain Appendix 2 – Bill of Material. The Commercial Bid should give all relevant price information and should not contradict the Pre-qualification and 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.

Evaluation Criteria

The competitive bids shall be submitted in two stages:

- ▶ Stage 1 – Eligibility cum Technical Evaluation
- ▶ Stage 2– Commercial Evaluation

6.4 Eligibility cum Technical Evaluation

The Technical bids of bidders qualifying the eligibility criteria will be opened and reviewed to determine whether the technical bids are substantially responsive. Bids that are not substantially responsive are liable to be disqualified at OICL'S discretion.



The technical soundness of Bidder's proposals will be rated as follows:

S. No.	Evaluation Criteria	Maximum Marks	Minimum Marks	Minimum Passing Percentage
1.	Compliance to Scope of Work	100	100	100%
2.	Compliance to Technical Specifications	100	100	100%
3.	Past Experience	100	75	75%
4.	Technical Presentation	200	150	75%
S. No.	Evaluation Criteria	Maximum Marks	Minimum Marks	Minimum Passing Percentage
	Total	500	425	85%

Bidders scoring at least the minimum score in each section mentioned in the table above and an overall score of 425 marks or more will be declared technically qualified.

The bidders scoring less than 425 marks (cut-off score) out of 500 marks in the technical evaluation shall not be considered for further selection process and their offers will be dropped at this stage. Bidders should score minimum as mentioned in the above table.

In case none of the participating bidders qualify on technical criteria by reaching or exceeding the cut off score of 85%, then OICL, at its sole discretion, may relax the cut-off score to a lower value, which, in any case, shall not fall below 75%. In case at-least two participants have not scored 75%, then OICL reserves the right to cancel and go for retendering process. However, this would be at the sole discretion of OICL.

OICL also reserves the right to conduct Reference Site Visits at the bidder's client sites or through call with client. Unsatisfactory/ negative feedback during site visit will lead to outright rejection of bid.

The evaluation of technical proposals, among other things, will be based on the following:

S.No.	Technical Evaluation	Evaluation Methodology								
1	Compliance to Scope of Work Max. Marks- 100 marks	The Bidder is required to submit an undertaking stating 100% Compliance to Scope of Work mentioned in this detailed document. Note: <i>Deviations and non-conformance to scope of work will lead to disqualification.</i>								
2	Compliance to Technical Specifications Max. Marks- 100 marks	The Bidder is required to submit compliance to Technical Specifications. Bidders should score 100% in Compliance to Specifications (Appendix 1). Marks would be awarded as: <table><tr><th>Status</th><th>Marks</th></tr><tr><td>Yes</td><td>10</td></tr><tr><td>No</td><td>0</td></tr></table> The total marks of the Appendix will be scaled down on a scale of 100 marks			Status	Marks	Yes	10	No	0
Status	Marks									
Yes	10									
No	0									
4	Bidder’s Past Experience	Category	No. of Credentials	Marks						



of having supplied, implemented and maintained/maintaining: Max. Marks- 100 marks	Proposed EMS solution with at least 7,500 employees	In at least one BFSI /PSU/Government Organization in India	40
		More than one BFSI/PSU/Government Organization in India	50
	Endpoint Security with at least 7,500 endpoints	In at least one BFSI/PSU/Government Organization in India	35
		More than one BFSI/PSU/Government Organization in India	50

S.No.	Technical Evaluation	Evaluation Methodology
3	Technical Presentation Max. Marks- 200 marks	All eligible bidders will be required to make presentations. OICL will schedule presentations and the time and location will be communicated to the bidders. Failure of a bidder to complete a scheduled presentation to OICL may result in rejection of the proposal. Marks will be scored on the following points: <ol style="list-style-type: none">1. Overall understanding of Scope & Requirements2. Demonstration of organization's capability for the proposed initiative3. Service Model Demonstration4. Demonstration of value proposition offered in the bid which shall enable the success of the project5. Detailed Solution Capability and Implementation approach6. Ability to respond to OICL's queries

The commercial proposals of technically short-listed Bidders will then be opened.

6.5 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 Six (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.

Bidder to note that Appendix-2: Bill of Material with complete bifurcation of Price which is mentioned in GEM Portal (As a consolidated Price) needs to submit at OICL Office (address mentioned in RFP). This needs to be submitted with proper labelling, seal, sign and stamped.

Bidder to note that the appendix needs to be submitted physically on the same date and time which is the RFP submission date and time.



If any Bidder fails to submit the same the bid will be rejected.

Bidder needs to note that Amount (consolidated amount on GEM Portal) and the total of bifurcation mentioned in the Appendix-2 Bill of material has to be tally till 2 decimal places. If any discrepancy found that bid will be rejected.

7 Service Level Agreement

OICL intends to select the Successful Bidder who shall have common vision to deliver high quality of services to the users.

Definition of terms used in this section is as follows:

1. **"Downtime"** shall mean the time period for which the specified services / components with specified technical and service standards are not available to OICL and excludes the scheduled outages planned in advance and the bandwidth link failures
2. **"Incident"** refers to any event / abnormalities in the functioning of the equipment / specified services that may lead to deterioration, disruption in normal operations of OICL's services.
3. **"Resolution Time"** shall mean the time taken in resolving (diagnosing, trouble shooting and fixing) an incident after it has been reported at the helpdesk. The resolution time shall vary based on the category of the incident reported at the service desk. The category shall be defined and agreed between OICL and Service Provider.
4. **"Scheduled operation time"** means the scheduled operating hours of the System for the month. All planned downtime on the system would be deducted from the total operation time for the month to give the scheduled operation time, i.e. 24x7x365.
5. **"Solution downtime"** subject to the SLA, means accumulated time during which the Solution is not available to OICL's users or customers due to in-scope system, and measured from the time OICL and/or its customers log a call with the Bidder help desk of the failure or the failure is known to the Bidder from the availability measurement tools to the time when the System is returned to proper operation. Any denial of service to OICL's users and OICL's customers would also account as "System downtime"
6. The business hours are 9 AM to 6 PM on any calendar day OICL is operational. The Bidder however recognizes the fact that the branches will require to work beyond the business hours and holidays on need basis.
7. Uptime will be computed based on availability of the applications to OICL's users irrespective of availability of servers either individual servers/clusters.
8. Typical Resolution time will be applicable if systems are not available to OICL's users and customers and there is a denial of service.
9. Bidder to note that all SLAs will be applicable 3 months post Go-Live onwards.

7.1.1 Service Level Agreement and Targets

This section includes the SLAs which OICL requires the Successful Bidder to manage as key performance indicators for the scope of work. The objective of the SLA is to clearly define the levels of services to be delivered by the Successful Bidder to OICL for the duration of the contract.

The following section reflects the measurements to be used to track and report performance on a regular basis.

The targets shown in the following sections are for the period of contractor its revision whichever is earlier.



Service Level Availability is to be measured and reported on a monthly basis by bidder and will be validated by BOM.

System Availability is defined as:

$$\{(\text{Scheduled Operation Time} - \text{System Downtime}) / (\text{Scheduled Operation Time})\} * 100\%$$

7.1.2 Service Level Measurement

1. OICL has defined in-scope services in the RFP and corresponding SLAs below. OICL shall evaluate the performance of the Successful Bidder on these SLAs compliance as per the periodicity defined.
2. The Successful Bidder shall provide, as part of monthly evaluation process, reports to verify the Successful Bidder's performance and compliance with the SLAs. Data capturing and reporting mechanism will be used for SLA reporting. The bidder has to leverage existing tools or any other tool proposed by OICL to monitor and manage the Solution.
3. If the level of performance of Successful Bidder for a particular metric fails to meet the minimum service level for that metric, it will be considered as a Service Level Default.
4. The Bidder shall provide SLA Report on monthly basis and a review shall be conducted based on this report. A monthly report shall be provided to OICL at the end of every month containing the summary of all incidents reported and associated Bidder performance measurement for that period. Performance measurements would be accessed through audits or reports, as appropriate to be provided by the Bidder.

7.1.3 Availability

Services	Description	Calculation	Periodicity	MSL	Penalty
Solution Availability	Availability of Solution to users	(Total uptime in a month)/ (maximum time in a month - scheduled downtime)	Monthly	99.50%	For every 0.1% or part thereof drop in service levels penalty will be 1% of the total Facilities Management Cost for the quarter The Calculation of penalty will happen based quarterly performance data as received
Bug Resolution					



Bug Reporting	Bidder shall ensure that all bugs reported by the users / testing team shall be duly logged and assigned a unique ID for reference purposes. Users shall be informed about the reference ID maximum within 15 minutes from recording the complaint	Manually through various communication channels	Monthly	100%	Penalty of INR 1,000 will be levied for every 15 minutes delay or part thereof
Bug Resolution	Bidder shall ensure that all bugs reported by the users / testing	NA	Monthly	Per Instance	Penalty of INR 10,000 will be levied for every day delay or part
Services	Description	Calculation	Periodicity	MSL	Penalty
	team as agreed with OICL and resolved maximum within 7 calendar days. The reference ID post resolution should be closed in concurrence with OICL				thereof

7.1.4 Management, Reporting and Governance

Service Details	SLA Measurement	SLA	Penalty
Report Generation	Adherence to delivery of SLA report	100%	The SLA reports to be shared with OICL by 10 th of every month. For each default the penalty of INR 10,000 per week or part thereof maybe charged to the bidder
Staff transition period (Handover period)	Yearly 1 change in the Project Manager or Service delivery manager is allowed	100%	More than 1 change in the proposed Program Manager or Service delivery manager would lead to penalty of INR 5,000 for each default



Resource Availability	Resource availability for the contract period	No. of days below minimum attendance level	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)
-----------------------	---	--	---

7.1.5 Support/ Maintenance Matrix

The table below specifies support/maintenance matrix along with mean time to respond (MTTR1) and mean time to resolve (MTTR2). This is in addition to the penalty imposed for Availability.

#	Service	MTTR1	MTTR2	Penalty
1	Software Application (EMS/AD/AV/Help Desk)	10 minutes	Should maintain 99.5% uptime	INR 5,000 per day
2	AV signature updation (Bulk Update)		One day	INR 5,000 per day
3	Case logged to FMS from HO (Bulk Issues Case Log)	15 minutes	One Day	INR 5,000 per day

Note:

- SLA window for line item 3 will be 9.AM to 6 PM (Monday – Friday).
- 95 % of the user login, apart from one time profile creation should happen within 5 seconds. Nonadherence to the same will lead to penalty as per the SLA clause (7.1.3 Solution Availability) will be used to calculate downtime.
- MTTR1 (Mean Time to Response): Defined as time taken by the help desk to respond the concerned user over the service desk tool, phone/Email/FAX or in person and acknowledge the problem.
- MTTR2 (Mean Time to Resolve): Defined as time taken to resolve a problem.
- Bidder shall not be responsible for any issues related to respective OEM/ AMC Vendors/ Bandwidth.

Penalties

OICL reserves the right to recover the penalty from any payment to be made under this contract. The penalty would be deducted from the payouts. For the purpose of this RFP, the total of penalties as per SLA and the Liquidated damages will be subject to a maximum of 10% of the overall contract value.

At-Risk Amount

The monthly At-Risk Amount ('ARA') shall be 10% of the estimated monthly payout of the respective month. Overall cap for penalties as per SLA and the Liquidated damages over the tenure of the contract will be 10% (ten per cent.) of the contract value.

7.1.6 Exception

OICL shall not hold the Successful Bidder responsible for a failure to meet any Service Level if it is directly attributable to:



- i Execution of the disaster recovery plan/business continuity plan for an OICL declared disaster situation; and
- ii Any established inability of other third-party vendor or service provider of OICL, to fulfill the requirements as per the contract.

8 Disclaimer

This RFP is being issued by OICL for inviting bids for Selection of Vendor for Supply, Installation, & Maintenance of Desktop & IT Services Management Solution (DITSM) including Active Directory, Antivirus and Helpdesk Solution. 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.

9 Annexure

**This Page is
Intentionally
Left blank**



9.1 Annexure 1: Application form for Eligibility Bid

To
The Deputy General Manager
The Oriental Insurance Company Limited
Information Technology Department,
NBCC Office Complex, East Kidwai Nagar,
2nd Floor, Office Block 4,
New Delhi- 110023

Application form for the Eligibility of the Bidder

Tender Ref. No. OICL/HO/ITD/DITSM/2022/01

Company Details

1	Registered Name, Date and Address of the Bidder.	
2	Location of Corporate Headquarters.	
3	GST Identification No. and Date of Registration	
4	Address for Communication	
5	Contact Person 1 (Name, Designation, Phone, Email ID)	
6	Contact Person 2 (Name, Designation, Phone, Email ID)	

Turnover and Net worth

Financial Year	Turnover (Rs. in Crores)	Net worth



Name: _____
Designation: _____
Date: _____
Signature: _____ Company
Seal

9.2 Annexure 2: Technical Experience Details and Reference Form

Tender Ref. No. OICL/HO/ITD/DITSM/2022/01

Please attach supporting credentials for each reference provided.

S.No.	Name of Client	Financial Year	Contact Details of Client	Details of Project	Date of Award of Project	Current Status of Project

Signature: _____

Name: _____

Designation: _____

Date: _____

(Company Seal)

9.3 Annexure 3: Contract Form

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

WHEREAS the Purchaser is desirous that certain software, hardware and services should be provided by the Vendor viz., _____ and has accepted a bid by the Vendor for the supply of those hardware, 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.

RFP Document and corresponding Amendments (Reference No: **OICL/HO/ITD/DITSM/2022/01** Dated)

The Schedule of Requirements and the Requirement Specifications

The Service Level Agreement

The General Conditions of Contract

The Purchaser’s Notification of Award (PO Reference No.: _____)

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

The purchaser hereby covenants to pay the Vendor in consideration of the provision of the 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 Vendor, are as under:

Total Value in words: _____

Total Value: _____

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 _____
Name _____
Designation _____
Address _____
Company _____
Date _____

Signature _____
Name _____
Designation _____
Address _____
Company _____
Date _____

**Company Seal
Witness I**

**Company Seal
Witness II**



Signature	_____	Signature	_____
Name	_____	Name	_____
Designation	_____	Designation	_____
Address	_____	Address	_____
Company	_____	Company	_____
Date	_____	Date	_____



9.4 Annexure 4: Query Format

All pre-bid queries are to be sent in the following format:

S.No.	Page #	Point/ Section #	Existing Clause	Query Sought



9.5 Annexure 5: Bid Security Declaration

To
The Deputy General Manager
The Oriental Insurance Company Limited
Information Technology Department,
NBCC Office Complex, East Kidwai Nagar,
2nd Floor, Office Block 4,
New Delhi- 110023

Sir,

Reg: Tender Ref No: OICL/HO/ITD/DITSM/2022/01 I/We,

the undersigned, declare that:

I/We understand that, according to your conditions, bids must be supported by a Bid Securing Declaration.

I/We accept that I/We may be disqualified from bidding for any contract with you for a period of one year from the date of notification if I am /We are in a breach of any obligation under the bid conditions, because
I/We

- have withdrawn/modified/amended, impairs or derogates from the tender, my/our Bid during the period of bid validity specified in the form of Bid; or
- having been notified of the acceptance of our Bid by the purchaser during the period of bid validity (i) fail or refuse to execute the contract, if required, or (ii) fail or refuse to furnish the Performance Security, in accordance with the Instructions to Bidders.

I/We understand this Bid Securing Declaration shall cease to be valid if I am/we are not the successful Bidder, upon the earlier of (i) the receipt of your notification of the name of the successful Bidder; or (ii) thirty days after the expiration of the validity of my/our Bid.

Name: _____

Designation: _____

Date: _____

Signature: _____

Company Seal

9.6 Annexure 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..... 2022 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 theday of.....

Signature and Seal of Guarantors (Supplier's Bank)

.....

Date.....

Address.....

.....

9.7 Annexure 7: Statement of No Deviation

To

The Deputy General Manager

The Oriental Insurance Company Limited

Information Technology Department,

NBCC Office Complex, East Kidwai Nagar,

2nd Floor, Office Block 4,

New Delhi- 110023

Reference: Tender Ref No: OICL/HO/ITD/DITSM/2022/01

Sir,

There are no deviations (null deviations) from the RFP Requirements and Terms & Conditions of the tender. All the RFP Requirements and terms & conditions of the tender are acceptable to us.

Name: _____

Designation: _____

Date: _____

Signature: _____

Company Seal



9.8 Annexure 8: Office locations and service infrastructure facilities

Tender Ref. No. OICL/HO/ITD/DITSM/2022/01

Details of the Centre(s) owned and operated by the Bidder							
Name of City (located)	Address	Contact Person	Telephone Number(s)	Fax No.	E-mail address	Working hours	Remarks

Name: _____

Designation: _____

Date: _____

Signature: _____

Company Seal



9.9 Annexure 9: Bidder Profile

Tender Ref. No. OICL/HO/ITD/DITSM/2022/01

1.	Registered Name & Address of The Bidder	
2.	Location of Corporate Head Quarters	
3.	Date & Country of Incorporation	
4.	Service facilities location & size	
5.	Total number of employees	
6.	List of major clients	
7.	Name & Address of Contact Person with Tel. No / Fax /e-mail	
8.	Client Reference	
9.	Annual turnover for the three previous financial years	
10.	Net worth (Paid up capital plus free reserves) for the previous financial year (2021-22)	
11.	Name of the Authorized Signatory	

Name: _____

Designation: _____

Date: _____

Signature: _____

Company Seal

9.10 Annexure 10: Undertaking for providing authorized representatives of IRDAI the right to inspection, investigation, obtaining information

To
The Deputy General Manager
The Oriental Insurance Company Limited
Information Technology Department,
NBCC Office Complex, East Kidwai Nagar,
2nd Floor, Office Block 4,
New Delhi- 110023

Sir,

Reg: Undertaking from the Bidder for providing authorized representatives of the IRDAI the right to inspection, investigation, obtaining information for Tender Ref No: **OICL/HO/ITD/DITSM/2022/01**

We hereby undertake to provide authorized representatives of Insurance Regulatory Development Authority of India (IRDAI) right to:

- examine the books, records, information, systems and the internal control environment to the extent that they relate to the service being performed for the company and



- b) access to any internal audit reports or external audit findings for the service being performed for the company.

Name: _____

Designation: _____

Date: _____

Signature: _____

Company Seal

9.11 Annexure 11: Non-Disclosure Agreement

(On Rs.100 Non-Judicial stamp paper)

This Non-Disclosure Agreement made and entered into at..... This ... day of..... 202_

BY AND BETWEEN

..... Company Limited, a company incorporated under the

Companies Act, 1956 having its registered office at (Hereinafter referred to as the Vendor which expression unless repugnant to the context or meaning thereof be deemed to include its permitted successors) of the ONE PART;

AND

The Oriental Insurance Company Ltd, having its headquarter and Corporate Office at Information Technology Department, NBCC Office Complex, East Kidwai Nagar, 2nd Floor, Office Block 4, New Delhi- 110023 (hereinafter referred to as "OICL" which expression shall unless it be repugnant to the subject, meaning or context thereof, be deemed to mean and include its successors and assigns) of the OTHER PART. The Vendor and The Oriental Insurance Company Ltd are hereinafter collectively referred to as "the Parties" and individually as "the Party" WHEREAS:

1. The Oriental Insurance Company Ltd is engaged in the business of providing financial services to its customers and intends to engage Vendor for providing

2. In the course of such assignment, it is anticipated that The Oriental Insurance Company Ltd or any of its officers, employees, officials, representatives or agents may disclose, or deliver, to the Vendor some Confidential Information (as hereinafter defined), to enable the Vendor to carry out the aforesaid assignment (hereinafter referred to as "the Purpose").

3. The Vendor is aware and confirms that all information, data and other documents made available in the RFP/Bid Documents/Agreement /Contract or in connection with the Services rendered by the Vendor are confidential information and are privileged and strictly confidential and or proprietary of The Oriental Insurance Company Ltd. The Vendor undertakes to safeguard and protect such confidential information as may be received from The Oriental Insurance Company Ltd



NOW, THEREFORE THIS AGREEMENT WITNESSED THAT in consideration of the above premises and the Oriental Insurance Company Ltd granting the Vendor and or his agents, representatives to have specific access to The Oriental Insurance Company Ltd property / information and other data it is hereby agreed by and between the parties hereto as follows:

1. Confidential Information:

(i) "Confidential Information" means and includes all information disclosed/furnished by The Oriental Insurance Company Ltd to the Vendor whether orally, in writing or in electronic, magnetic or other form for the limited purpose of enabling the Vendor to carry out the proposed Implementation assignment, and shall mean and include data, documents and information or any copy, abstract, extract, sample, note or module thereof, explicitly designated as "Confidential"; Provided the oral information is set forth in writing and marked "Confidential" within seven (7) days of such oral disclosure.

(ii) The Vendor may use the Confidential Information solely for and in connection with the Purpose and shall not use the Confidential Information or any part thereof for any reason other than the Purpose stated above.

Confidential Information in oral form must be identified as confidential at the time of disclosure and confirmed as such in writing within seven (7) days of such disclosure. Confidential Information does not include information which:

- (a) is or subsequently becomes legally and publicly available without breach of this Agreement by either party,
- (b) was rightfully in the possession of the Vendor without any obligation of confidentiality prior to receiving it from The Oriental Insurance Company Ltd,
- (c) was rightfully obtained by the Vendor from a source other than The Oriental Insurance Company Ltd without any obligation of confidentiality,
- (d) was developed by for the Vendor independently and without reference to any Confidential Information and such independent development can be shown by documentary evidence, or is/was disclosed pursuant to an order of a court or governmental agency as so required by such order, provided that the Vendor shall, unless prohibited by law or regulation, promptly notify The Oriental Insurance Company Ltd of such order and afford The Oriental Insurance Company Ltd the opportunity to seek appropriate protective order relating to such disclosure.
- (e) the recipient knew or had in its possession, prior to disclosure, without limitation on its confidentiality.
- (f) is released from confidentiality with the prior written consent of the other party.

The recipient shall have the burden of proving hereinabove are applicable to the information in the possession of the recipient. Confidential Information shall at all times remain the sole and exclusive property of the disclosing party. Upon termination of this Agreement, Confidential Information shall be returned to the disclosing party or destroyed, if incapable of return. The destruction shall be witnessed and so recorded, in writing, by an authorized representative of each of the parties.

Nothing contained herein shall in any manner impair or affect rights of The Oriental Insurance Company Ltd in respect of the Confidential Information.

In the event that any of the Parties hereto becomes legally compelled to disclose any Confidential Information, such Party shall give sufficient notice to the other party to enable the other Party to prevent or minimize to the extent possible, such disclosure. Neither party shall disclose to a third party any Confidential Information or



the contents of this Agreement without the prior written consent of the other party. The obligations of this Clause shall be satisfied by handling Confidential Information with the same degree of care, which the receiving party applies to its own similar confidential information but in no event less than reasonable care.

The obligations of this clause shall survive the expiration, cancellation or termination of this Agreement

2. Non-disclosure: The Vendor shall not commercially use or disclose any Confidential Information, or any materials derived there from to any other person or entity other than persons in the direct employment of the Vendor who have a need to have access to and knowledge of the Confidential Information solely for the Purpose authorized above. The Vendor shall take appropriate measures by instruction and written agreement prior to disclosure to such employees to assure against unauthorized use or disclosure. That a copy of the agreement shall also be given to OICL. The Vendor may disclose Confidential Information to others only if the Vendor has executed a Non-Disclosure Agreement with the other party to whom it is disclosed that contains terms and conditions that are no less restrictive than these presents and the Vendor agrees to notify The Oriental Insurance Company Ltd immediately if it learns of any use or disclosure of the Confidential Information in violation of terms of this Agreement.

Notwithstanding the marking and identification requirements above, the following categories of information shall be treated as Confidential Information under this Agreement irrespective of whether it is marked or identified as confidential:

- a) Information regarding The Oriental Insurance Company Ltd and any of its Affiliates, customers and their accounts ("Customer Information"). For purposes of this Agreement, Affiliate means a business entity now or hereafter controlled by, controlling or under common control. Control exists when an entity owns or controls more than 10% of the outstanding shares or securities representing the right to vote for the election of directors or other managing authority of another entity; or
- b) any aspect of The Oriental Insurance Company Ltd business that is protected by patent, copyright, trademark, trade secret or other similar intellectual property right; or
- c) business processes and procedures; or
- d) current and future business plans; or
- e) personnel information; or
- f) financial information.

3. Publications: The Vendor shall not make news releases, public announcements, give interviews, issue or publish advertisements or publicize in any other manner whatsoever in connection with this Agreement, the contents / provisions thereof, other information relating to this Agreement, the Purpose, the Confidential Information or other matter of this Agreement, without the prior written approval of The Oriental Insurance Company Ltd.

4. Term: This Agreement shall be effective from the date hereof and shall survive the expiration, cancellation or termination of this Agreement.

The Vendor hereby agrees and undertakes to The Oriental Insurance Company Ltd that immediately on termination of this Agreement it would forthwith cease using the Confidential Information and further promptly return or destroy, under information to The Oriental Insurance Company Ltd, all information received by it from The Oriental Insurance Company Ltd for the Purpose, whether marked Confidential or otherwise,



and whether in written, graphic or other tangible form and all copies, abstracts, extracts, samples, notes or modules thereof. The Vendor further agree and undertake to The Oriental Insurance Company Ltd to certify in writing upon request of The Oriental Insurance Company Ltd that the obligations set forth in this Agreement have been complied with.

Any provisions of this Agreement which by their nature extend beyond its termination shall continue to be binding and applicable without limit in point in time except and until such information enters the public domain

5. Title and Proprietary Rights: Notwithstanding the disclosure of any Confidential Information by The Oriental Insurance Company Ltd to the Vendor, the title and all intellectual property and proprietary rights in the Confidential Information shall remain with The Oriental Insurance Company Ltd.

6. Remedies: The Vendor acknowledges the confidential nature of Confidential Information and that damage could result to The Oriental Insurance Company Ltd if the Vendor breaches any provision of this Agreement and agrees that, if it or any of its directors, officers or employees should engage or cause or permit any other person to engage in any act in violation of any provision hereof, The Oriental Insurance Company Ltd may suffer immediate irreparable loss for which monetary compensation may not be adequate. The Oriental Insurance Company Ltd shall be entitled, in addition to other remedies for damages & relief as may be available to it, to an injunction or similar relief prohibiting the Vendor, its directors, officers etc. from engaging in any such act which constitutes or results in breach of any of the covenants of this Agreement.

Any claim for relief to The Oriental Insurance Company Ltd shall include The Oriental Insurance Company Ltd costs and expenses of enforcement (including the attorney's fees).

7. Entire Agreement, Amendment and Assignment: This Agreement constitutes the entire agreement between the Parties relating to the matters discussed herein and supersedes any and all prior oral discussions and / or written correspondence or agreements between the Parties. This Agreement may be amended or modified only with the mutual written consent of the Parties. Neither this Agreement nor any right granted hereunder shall be assignable or otherwise transferable.

8. Governing Law: The provisions of this Agreement shall be governed by the laws of India and the competent court at Delhi shall have exclusive jurisdiction in relation thereto.

9. Indemnity: The Vendor shall defend, indemnify and hold harmless The Oriental Insurance Company Ltd, its affiliates, subsidiaries, successors, assigns, and their respective officers, directors and employees, at all times, from and against any and all claims, demands, damages, assertions of liability whether civil, criminal, tortuous or of any nature whatsoever, arising out of or pertaining to or resulting from any breach of representations and warranties made by the Vendor. and/or breach of any provisions of this Agreement, including but not limited to any claim from third party pursuant to any act or omission of the Vendor, in the course of discharge of its obligations under this Agreement.

10. General: The Vendor shall not reverse - engineer, decompile, disassemble or otherwise interfere with any software disclosed hereunder.

All Confidential Information is provided "as is". In no event shall the Oriental Insurance Company Ltd be liable for the inaccuracy or incompleteness of the Confidential Information. None of the Confidential Information disclosed by The Oriental Insurance Company Ltd constitutes any representation, warranty, assurance, guarantee or inducement with respect to the fitness of such Confidential Information for any particular purpose.



The Oriental Insurance Company Ltd discloses the Confidential Information without any representation or warranty, whether express, implied or otherwise, on truthfulness, accuracy, completeness, lawfulness, merchantability, and fitness for a particular purpose, title, non-infringement, or anything else.

11. Waiver: A waiver (whether express or implied) by The Oriental Insurance Company Ltd of any of the provisions of this Agreement, or of any breach or default by the Vendor in performing any of the provisions hereof, shall not constitute a continuing waiver and such waiver shall not prevent The Oriental Insurance Company Ltd from subsequently enforcing any of the subsequent breach or default by the Vendor under any of the provisions of this Agreement.

In witness whereof, the Parties hereto have executed these presents the day, month and year first herein above written.

For and on behalf of ----- Ltd.

(_____)

(Designation)

For and on behalf of The Oriental Insurance Company Ltd

(_____)

(Designation)



9.12 Annexure 12: Integrity Pact

(On Rs.100 Non-Judicial stamp paper)

PRE-CONTRACT INTEGRITY PACT

General

This pre-bid pre contract Agreement (hereinafter called the integrity pact is made on day of the month of _____202_, between, on one hand, The Oriental Insurance Company Ltd, having its headquartered and Corporate Office at NBCC Office Complex, East Kidwai Nagar, 2nd Floor, Office Block 4, New Delhi- 110023, acting through _____, _____ (hereinafter called the “BUYER” which expression shall mean and include, unless the context otherwise requires, his successors in office and assignees) of the first part and M/s _____ represented by Shri _____, authorized signatory of M/s -----(hereinafter called the “BIDDER/SELLER” which expression shall mean and include, unless the context otherwise requires, his successors and permitted assigns)of the second part . WHEREAS the BUYER proposes to procure (Name of the Store /Equipment /item and the BIDDER /SELLER is willing to offer /has offered the store and

WHEREAS the BIDDER is a private company/public company/Government /undertaking/partnership/ registered export agency, constituted in accordance with the relevant law in the matter and the BUYER is a Government of India, Public Sector Insurance Company.

Now, THEREFORE,

To avoid all forms of corruption by following a system that is fair, transparent and free from any influence /prejudiced dealings prior to, during and subsequent to the currency of the contract to be entered into with a view to:-

Enabling the BUYER to obtain the desired said store/equipment at a competitive price in conformity with the defined specifications by avoiding the high cost and the distortionary impact of corruption on public procurement, and

Enabling the BIDDERS to abstain from bribing or indulging in any corrupt practice in order to secure the contract by providing assurance to them that their competitors will also abstain from bribing and other corrupt practices and the BUYER will commit to prevent corruption, in any form, by its officials by following transparent procedures.

The parties hereby agree to enter into this integrity pact and agree as follows: -

1. Commitments of the BUYER

1.1 The BUYER undertakes that no official of the BUYER, connected directly or indirectly with the contract, will demand, take a promise for or accept directly or accept, directly or through intermediaries, any bribe, consideration, gift, reward favor or any material or immaterial benefit or any other advantage from the BIDDER, either for themselves or for any person, organization or third party related to the contract in exchange for an advantage in the bidding process, bid evaluation contracting or implementation process related to the contract.



1.2 The BUYER will, during the pre- contract stage treat all BIDDERS alike, and will provide to all BIDDERS the same information and will not provide any such information to any particular BIDDER which could afford an advantage to that particular BIDDER in comparison to other BIDDERS.

1.3 All the officials of the BUYER will report to the appropriate Government office any attempted or completed breaches of the above commitment as well as any substantial suspicion of such a breach.

2. In case any such preceding misconduct on the part of such official (s) is reported by the BIDDER to the BUYER with full and verifiable facts and the same is prima facie found to be correct by the BUYER, necessary disciplinary proceedings, or any other action as deemed fit including criminal proceedings may be initiated by the BUYER and such a person shall be debarred from further dealings related to the contract process. In such a case while an enquiry is being conducted by the BUYER the proceedings under the contract would not be stalled.

3. Commitment of BIDDERS

The BIDDERS commit itself to all take all measures necessary to prevent corrupt practices, unfair means and illegal activities during any stage of its bid or during any pre-contract or post- contract stage in order to secure the contract or in furtherance to secure it and in particular commit itself to the following:-

3.1 The BIDDER will not offer, directly or through intermediaries, any bribe, gift, consideration, reward, favor, any material or immaterial benefit or other advantage, commission, fees, brokerage or inducement to any official of the BUYER, connected directly or indirectly with the bidding process, or to any person, organization or third party related to the contract in exchange for any advantage in the bidding, evaluation contracting and implementation of the contract.

3.2 The BIDDER further undertakes that it has not given, offered or promised to give, directly or indirectly any bribe, gift, consideration, reward, favor, any material benefit or other advantage commission fees, brokerage or inducement to any official of the BUYER or otherwise in procuring the contract forbearing to do or having done any act in relation to the obtaining or execution of the contract or any other contract with the Government for showing or for bearing to show favor or disfavor to any person in relation to the contract or any other contract with the Government.

3.3 BIDDERS shall disclose the name and address of agents and representatives and Indian BIDDERS shall disclose their foreign principals or associates.

3.4 BIDDERS shall disclose the payment to be made by them to agents/brokerage or any other intermediary, in connection with this bid/contract.

3.5 The BIDDER further confirms and declares to the BUYER that the BIDDER is the original manufacturer/integrator/authorized Government sponsored export entity of the has not engaged any individual or firm or company whether Indian or foreign to intercede, facilitate or in any way to recommend to the BUYER or any of its functionaries, whether officially or unofficially to the award of the contract to the BIDDER, nor has such any amount been paid promised or intended to be paid to any such Individual, firm or company in respect of any such intercession, facilitation or recommendation.

3.6 The BIDDER, either while presenting the bid or during pre- contract negotiations or before signing the contract shall disclose any payment he has made, is committed to or intends to make to officials of the BUYER or their family members agents, brokers or any other intermediaries in connection with the contract details or/and the services agreed upon for such payments.



3.7 The bidder will not collude with other parties interested in the contract to impair the transparency, fairness and progress of the bidding process, bid evaluation contracting and implementation of the contract.

3.8 The BIDDER will not accept any advantage in exchange for any corrupt practice, unfair means and illegal activities.

3.9 The BIDDER shall not use improperly, for purposes of competition or personal gain, or pass on to other, any information provided by the BUYER as part of the business deal, relationship regarding plans, technical proposals and business details, including information contained in any electronic data carrier. The BIDDER also undertakes to exercise due and adequate care lest any such information is divulged.

3.10 The BIDDER commits to refrain from giving any complaint directly or through any other manner without supporting it with full and verifiable facts.

3.11 The BIDDER shall not instigate or cause to instigate any third person to commit any of the action mentioned above.

3.12 The BIDDER will not, directly or through any other person or firm, offer, promise or give to any of the Principal's employees involved in the tender process or the execution of the contract or to any third person any material or other benefit which he/she is not legally entitled to, in order to obtain in exchange any kind of favor whatsoever during the tender process or during the execution of the contract.

4. Previous Transgression

4.1 The BIDDER declares that no previous transgression occurred in the last three year immediately before signing of this integrity pact, with any other company in any country in respect of any corrupt practices envisaged hereunder or with any public sector enterprise in India or any government Department in India that justify BIDDER'S exclusion from the tender process.

4.2 The BIDDER agrees that if it makes incorrect statement on this subject, BIDDER can be disqualified from the tender propose or the contract, if already awarded. Can be terminated for such reason.

5. Earnest money (security deposit)

5.1 While submitting commercial bid, the BIDDER shall submit a declaration as per format mentioned in the RFP for Earnest money/security.

5.2 The declaration against Earnest money / Security deposit shall be valid for the contract period or the complete conclusion of the contractual obligations to the complete satisfaction of both the BIDDER and the BUYER, including warranty period, whichever is later.

5.3 In case of the successful BIDDER a clause would also be incorporated in the article pertaining to performance bond in the purchase contract that the provisions of sanction for violation shall be applicable for, forfeiture of performance bond in case of a decision by the BUYER to forfeit the same without assigning any reason for imposing sanction for violation of this pact.

5.4 No interest shall be payable by the BUYER to the BIDDER on Earnest Money/Security Deposit for the period of its currency.



6. Sanctions for violations

6.1 Any breach of the aforesaid provisions by the BIDDER or anyone Employed by it or acting on its behalf (whether with or without the knowledge of the BIDDER) shall entitle the BUYER to take all or any one of the following actions, wherever required:

- (i) To immediately call off the pre contract negotiations without assigning any reason or giving any compensation to the BIDDER. However, the proceeding with the other BIDDER(s) would continue.
- (ii) The Earnest Money Deposit (in pre-contract stage) and/or Security Deposit /Performance bond (after the contract is signed shall stand forfeited either fully or partially, as decided by the BUYER and the BUYER shall not be required to assign any reason, therefore.
- (iii) To immediately cancel the contract, if already signed, without giving any compensation to the BIDDER.
- (iv) To recover all sum already paid by the BUYER, and in case of an Indian BIDDER with interest thereon at 2% higher than the prevailing prime lending rate of State Bank of India, while in case of a BIDDER from a country other than India with interest thereon at 2% higher than the LIBOR. If any outstanding payment is due to the BIDDER from the BUYER in outstanding payment could also be utilized to recover the aforesaid sum and interest.
- (v) To encash the advance bank guarantee and performance bond / warranty bond, if furnished by the BIDDER in order to recover the payments, already made by the BIDDER, along with interest.
- (vi) To cancel all or any other contracts with the BIDDER, the BIDDER shall be liable to pay compensation for any loss or damage to the BUYER resulting from such cancellation/ rescission and the BUYER shall be entitled to deduct the amount so payable from the money (s) due to the BIDDER.
- (vii) To debar the BIDDER from participating in future bidding processes of the Government of India for a minimum period of five year, which may be further extended at the discretion of the Buyer
- (viii) To recover all sum paid in violation of this pact by bidder (s) to any middleman or agent or broker with a view to securing the contract.
- (ix) In case where irrevocable letters of credit have been received in respect of any contract signed by the BUYER with the BIDDER, the same shall not be opened.
- (x) Forfeiture of performance bond in case of a decision by the BUYER to forfeit the same without assigning any reason for imposing sanction for violation of this pact.

6.2 The BUYER will be entitled to take all or any of the actions mentioned at Para 6.1(i) to (x) of this pact also on the commission by the BIDDER or any one employed by it or acting on its behalf (whether with or without the knowledge of the BIDDER), of an offence as defined in chapter IX of the Indian penal code, 1860 or prevention of corruption.

6.3 The decision of the BUYER to the effect that breach of the provisions of this pact has been committed by the BIDDER shall be final and conclusive on the BIDDER. However, the BIDDER can approach the independent monitor (s) appointed for the purpose of this pact.

7. Fall Clause

The BIDDER undertakes that it shall not supply similar Product / systems or subsystems in comparable business circumstances at a price lower than that offered in the present bid in respect of any other Public Sector Banks/Insurance Companies in India and if it is found that within one year after the signing of contract that



similar product / systems or sub systems is supplied by the BIDDER to any other Public Sector Banks/Insurance Companies in India at a lower price, with due allowance for elapsed time, will be applicable to the present case and the difference in the cost would be refunded by the BIDDER to the BUYER, if the contract has already been concluded.

8. Independent Monitors

8.1 The BUYER has appointed Independent Monitors (here either referred to as Monitors) for this pact in consulation with the central vigilance commission.

8.2 The task of the Monitors shall be to review Independent and objectively, whether and to what extent the parties comply with the obligations under this pact.

8.3 The Monitors shall not be subject to instruction by the representatives of the parties and perform their functions neutrally and independently.

8.4 Both the parties accept that the Monitors have the access to all the documents relating to the project/procurement, including minutes of meeting.

8.5 As soon as the monitor notice, or has reason to believe, a violation of this pact, he will so inform the Authority designated by the BUYER.

8.6 The BIDDER (s) accepts that the Monitor has the right to access without restriction to all project documentation of the BUYER including that provided by the BIDDER. The BIDDER will also grant the monitor, upon his request and demonstration of a valid interest, unrestricted and unconditional access to his project documentation. The same is applicable to subcontractors. The monitor shall be under contractual obligation to treat the information and documents of the BIDDER/subcontractor(s) with confidentiality.

8.7 The BIDDER will provide to the Monitor sufficient information about all meetings among the parties related to the project provided such meetings could have an impact on the contractual relations between the parties the parties will offer to the monitor the option to participate in such meetings.

8.8 The monitor will submit a written report to the designated Authority of BUYER / Secretary in the Department/ within 8 to 10 weeks from the date of reference or intimation to him by the BUYER/ BIDDER and, should the occasion arise, submit proposals for correcting problematic situations.

9. Facilitation of Investigation

In case of any allegation of violation of any provision of this pact or payment of commission, the BUYER or its agencies shall be entitled to examine all the documents including the Books of Accounts of the BIDDER and the BIDDER shall provide necessary information and documents in English and shall extend all possible help for the purpose of such examination.

10. Law and place of jurisdiction

This Pact is subject to Indian Law. The place of performance and jurisdiction shall be Delhi.

11. Other Legal Actions

The actions stipulated in this Integrity pact are without prejudice to any other legal action that may follow in accordance with provisions of the extent law in force relating to any civil or criminal proceedings.



12. Validity

12.1 The validity of this Integrity Pact shall be from date of this signing and extend up to 5 years or the complete execution of the contract to the satisfaction of both the BUYER and the BIDDER/SELLER. In case BIDDER is unsuccessful, this Integrity Pact shall expire after six months from the date of the signing of the contract.

12.2 Should one or several provisions of this Pact turn out to be invalid, the reminder of this Pact shall remain valid. In this case, the parties will strive to come to an agreement to their original intentions.

13. The BIDDER undertakes that he shall not approach the Court while representing the matter to External Independent Monitors (IEMs) and he will await their decision in the matter within a time ceiling of 90 days.

14. The parties hereby sign this Integrity Pact at _____ on _____

Signed, Sealed and Delivered for "The Oriental Insurance Company Ltd." By it's constituted Authority	Signed, Sealed and Delivered for M/s _____ by it's constituted Authority
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: _____



9.13 Annexure 13: Undertaking of Authenticity for Appliance and Equipment Supplies

RFP No: **OICL/HO/ITD/DITSM/2022/01**

Date:

To,
The Deputy General Manager
The Oriental Insurance Company Limited
Information Technology Department,
NBCC Office Complex, East Kidwai Nagar,
2nd Floor, Office Block 4,
New Delhi- 110023

Dear Sir,

With reference to the RFP for Selection of Vendor for Supply, Installation & Maintenance of Desktop & IT Services Management Solution (DITSM) including Active Directory, Antivirus and Helpdesk Solution will be supplied/quoted to you.

We hereby undertake that all the components/parts/assembly/software used shall be original new components/parts/assembly/software only, from respective OEMs of the products and that no refurbished/duplicate/second hand components/parts/ assembly / software are being used or shall be used.

We also undertake that in respect of hardware, software/solution/Operating system if asked for by you in the purchase order, the same shall be supplied along with the authorized license certificate (e.g. Product Keys on Certification of Authenticity) and also that it shall be sourced from the authorized source.

Should you require, we hereby undertake to produce the certificate from our OEM supplier in support of above undertaking at the time of delivery/installation. It will be our responsibility to produce such letters from our OEM supplier's at the time of delivery or within a reasonable time.

In case of default and we are unable to comply with above at the time of delivery or during installation, for the IT Hardware/Software already billed, we agree to take back the equipment, without demur, if already supplied and return the money if any paid to us by you in this regard.

Name: _____

Designation: _____

Date: _____

Signature: _____

Company Seal



9.14 Annexure 14: Manufacturers Authorization Format

(To be submitted on OEMs Letter Head)

[To be included in 'Cover – A' Eligibility Bid Envelope]

RFP No: **OICL/HO/ITD/DITSM/2022/01**

Date:

To,
Deputy General Manager
The Oriental Insurance Company Limited
Information Technology Department,
NBCC Office Complex, East Kidwai Nagar,
2nd Floor, Office Block 4,
New Delhi- 110023

Subject: Manufacturers Authorization Form Tender Ref No: **OICL/HO/ITD/DITSM/2022/01 Dated 09/12/2022**

<This MAF should be on the letterhead of the OEM and should be signed by a person competent and having the power of attorney to bind the manufacturer. It should be included by the bidder in its eligibility bid> MAF should broadly cover the following:

- a. Registered office address of OEM
- b. Authorizing bidder to participate in the tender and negotiate and conclude the contract with OICL.
- c. Confirm extension of full warranty and guarantee as per the terms and conditions of the tender and the contract for the solution, products/equipment and services including extension of technical support and updates / upgrades if contracted by the bidder.
- d. Ensure all product upgrades including software upgrades and new product feature releases during the contract period.
- e. And also confirm that such Products as OICL may opt to purchase from the Supplier/Bidder, provided, that this option shall not relieve the Supplier/Bidder of any warranty obligations under the Contract.
- f. In the event of termination of production of such Products:
 - i. advance notification to OICL of the pending termination, in sufficient time to permit the OICL to procure needed requirements; and
 - ii. Following such termination, furnishing at no cost to OICL, the blueprints, design documents, operations manuals, standards and specifications of the Products, if requested.
- g. Should also confirm to undertake, that in case if the bidder is not able to maintain the solution to the satisfaction of the Company as per the functional and technical specification of the bid, will replace the bidder with another bidder to maintain the solution till the contract period in this bid at no extra cost to the company.

Yours faithfully,

(Authorized Signatory of Bidder)

Date:



(Company Seal)

9.15 Annexure 15: Undertaking from OEM for Equipment Supplies on time

RFP No: OICL/HO/ITD/DITSM/2022/01

Date:

To,
The Deputy General Manager
The Oriental Insurance Company Limited
Information Technology Department,
NBCC Office Complex, East Kidwai Nagar,
2nd Floor, Office Block 4,
New Delhi- 110023

Dear Sir,

With reference to the Hardware and software quoted in bid.

We hereby undertake that all the Hardware and software used shall be supplied as per Project Timelines from the PO issuance.

Name: _____

Designation: _____

Date: _____

Signature: _____

Company Seal

10 Appendix

10.1 Appendix 1: Technical Specifications

Anti-Virus with EDR

#	Particulars	Bidder's Compliance (Yes/No)	Remarks
1	General		
1.1	The proposed solution should be purpose build, unified agent for all features with on-premise architecture		
1.2	The proposed solution shall be licensed for at least 10,000 client machines		
1.3	The proposed solution client shall be loaded on the endpoints and the server shall distribute the updates to the clients		



1.4	The proposed solution shall provide a Central Management dashboard to manage the entire solution		
1.5	- Solution must provide central management functions in terms of logs, threat intelligence, status of managed products/devices		
1.6	- Central management should work as centralized threat sharing/management server with the managed clients		
1.7	- Solution should be able to provide a central view of threat detections for managed devices		
1.8	- Solution should be able to generate downloadable reports from existing and customizable templates		
1.9	The proposed solution should be deployed in centralized architecture to manage policies and should be controlled centrally.		
1.10	The proposed solution should support the following Operating Systems Platforms- Windows 8, Windows 10, Windows 11, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 or Latest, RHEL and Cent OS.		
1.11	The proposed solution should have the following protection mechanism:		
1.11.1	Anti-Malware, anti-ransomware protection		
1.11.2	Host Intrusion Prevention System / Anti exploit module		
1.11.3	Application Control & Disk encryption		
1.11.4	Zero Phishing & end point compliance		
1.11.5	Endpoint Detection & Response		
1.12	The proposed solution shall offer all the features specified herein in a single unified installation. Installation of multiple agents to achieve the requirement is not acceptable.		
1.13	The proposed solution shall provide following installation methods:		

#	Particulars	Bidder's Compliance (Yes/No)	Remarks
1.13.1	a) EXE/MSI Package based installer		
1.13.2	b) Web based installation		
1.13.3	c) Login script based installation		
1.13.4	d) Remote installation		
1.13.5	e) Through AD or through proposed EMS		



1.14	All the client components should be installed using the single client package Deployment tool if required, for end point rollout will be responsibility of bidder		
1.15	The proposed solution should prevent normal user from uninstalling the endpoint security client		
1.16	The proposed solution shall provide detection of endpoints that do not have the agent installed		
2	Malware Protection		
2.1	The proposed solution must protect against all kinds of viruses, Trojans and worms including but not limited to: boot sector, master boot sector, memory resident, macro, stealth and polymorphism etc.; and any other forms of exploits		
2.2	The proposed solution shall also protect against certain non-virus threats, such as Spyware, adware, dialers, joke programs, remote access and hacking tools, which can be used with malicious intent		
2.3	The solution will leverage multiple sensors to effectively and uniquely identify generic malware behaviors as well as malware family specific behaviors.		
2.4	The proposed solution should be able to do full scan of files / folders with a choice of specifying directories and file extensions not to be scanned		
2.5	The proposed solution should provide performance control while scanning files/folders/Hard disk		
2.6	The solution will identify and block out-going communication to malicious C&C sites. Cloud threat intelligence resources will be used for updates and identification of zero-day C&C attacks		
2.7	The proposed solution should provide behavioral analysis using machine learning and artificial intelligence to detect and mitigate emerging unknown security threats, which does not have any signatures		
2.8	The proposed solution should identifies the latest web browser exploits and prevents the exploits from being used to compromise the web browser		
2.9	The proposed solution shall inspect applications, as well as the applications' sub-components (DLLs) as they are executed		

#	Particulars	Bidder's Compliance (Yes/No)	Remarks
---	-------------	------------------------------	---------



2.10	The solution will enforce endpoint computers to comply with security rules that are defined for the organization. Computers that do not comply will be shown as non-compliant and can apply restrictive policies to them.		
2.11	The proposed solution on detection of a malware infection, should allow removal of traces of malware from the system by cleaning up the following automatically or via remote remediation console from centralized Management console:		
2.11.1	a) Detected malicious file		
2.11.2	b) Affected registry entries		
2.11.3	c) any new files dropped by malware		
2.11.4	d) windows services created by malware		
2.11.5	e) any other system settings affected by malware.		
2.12	The proposed solution shall ransomware protection against unauthorized encryption or modification		
2.13	The proposed solution shall protect against fileless malware and shall utilize behavioural techniques to detect malware based on the behaviour of the file		
2.14	The proposed solution should have tamper protection against malware that attempt to disable security measures		
2.15	The proposed solution should store event data at endpoint client while it is disconnected from the corporate network and forwards it on reconnection		
2.16	The proposed solution shall provide detection and blocking of Command and control (C&C) traffic and prevent access of malicious and dangerous websites		
2.17	The proposed solution must provide application of enforcement actions based on malicious file types such as Delete, Block, Quarantine		
2.18	Preventive controls from advanced sophisticated attack against users including Anti Phishing, Web form protection, account takeover protection etc.		
2.19	Solution must detect and block access to phishing sites by scanning all form fields. Solution should not be only dependent on url reputation based Techniques to identify phishing URL's :		
2.20	Full disk encryption - All volumes of the hard drive and hidden volumes are automatically fully encrypted. This includes system files, temporary files, and even deleted files.		
3	Anti-Exploit, Anti Ransomware Protection		



3.1	The proposed solution shall protect the endpoint against the exploitation of vulnerabilities in operating system and other applications		
-----	---	--	--

#	Particulars	Bidder's Compliance (Yes/No)	Remarks
3.2	The solution will protect against zero-day ransomware without requiring signature updates. The solution will remediate and restore files that were encrypted during a ransomware attack. Should have capability to identify and trace malicious ransomware payloads and PowerShell obfuscated code injections into memory & registry.		
3.3	The proposed solution must provide the flexibility to create firewall rules for controlling in bound and out bound rules to filter connections by IP address, port number, or protocol, and then apply the rules to different groups of users		
3.4	The solution will protect against existing and zeroday ransomware without requiring signature updates. The anti-ransomware capability should have auto rollback feature to restore the system back to original state. The anti-ransomware solution has third party-validation.		
3.5	Solution should support zero trust policy for files downloaded from untrusted sources on web. Solution must sanitize all the active content / scripts from the file before it deliver to end user.		
4	Application Control & Encryption		
4.1	The proposed solution provides a capable allow or deny policy that is able to manage known and unknown applications, file types, and executables		
4.2	The solution should allow for selection of Native encryption or BitLocker Management via policy.		
4.3	The solution should support seamless switching between BitLocker Management and Native encryption via policy.		
4.4	The proposed solution is able to provide a reliable file reputation source and global usage details to allow cross checking of known good files. This source must be constantly kept up- to-date with the latest known good file listing		
4.5	The solution will be used to restrict network access for specified applications. The Endpoint Security administrator defines policies and rules that allow, block or terminate applications and processes		



5	Device Control		
5.1	The proposed solution shall have the capability to control usage of external devices including storage devices, Non-storage devices etc. on the endpoint		
5.2	The proposed solution should potentially block the endpoint system from loading physical devices on USB bus such as removable storage devices, Bluetooth, Wi-Fi network cards etc.		

#	Particulars	Bidder's Compliance (Yes/No)	Remarks
5.3	The proposed solution shall provide management of storage devices and allow restrictions on their usage to Monitor, Block or make the device ReadOnly along with the option of providing exceptions		
5.4	The proposed solution shall allow usage of authorized USB devices by users and blocking of unauthorized USB devices. The solution shall allow exclusion of authorized USB devices by using their vendor ID, product ID or serial number		
5.5	The proposed solution shall provide logs of the device control feature to detect attempts of connecting unauthorized devices		
6	Security Definition Updates		
6.1	The proposed solution OEM should have a 24/7 security service update and should support real time updates of the system on release		
6.2	The proposed solution shall have an updating mechanism using local update server		
6.3	The proposed solution shall allow for incremental update of definitions		
6.4	The proposed solution shall provide a mechanism for updates of roaming devices or clients which are connected to Internet		
7	Management and Reporting		
7.1	The proposed solution should provide a management dashboard to view the status of endpoints across the enterprise locations/geographies and a central incident response to work on EDR/XDR features like detection models, threat hunting and response actions etc.		



7.2	The proposed solution shall offer enterprise-wide visibility over the status of all the deployed components. The dashboard shall provide a summarized view to analyse top threats & summary of malware traffic or any other threats		
7.3	Solution must continuously collect system events necessary for detection and analysis. Vendor must list specific items that are collected in real-time. (Data collected through post-event scripts or live interaction with host is covered in a separate requirement.) Examples must include, but not limited to, process events, file & registry modifications, network connections, cross-process activity, command line arguments, windows events, DNS queries and responses		
7.4	The proposed solution shall provide hierarchical grouping of machines and policy deployment		

#	Particulars	Bidder's Compliance (Yes/No)	Remarks
7.5	The proposed solution shall offer a central repository of the updates that can be distributed to the managed components		
7.6	The proposed solution should have minimum log retention period of upto 180 days		
7.7	The proposed solution shall be able to receive logs from the managed components and endpoints and store them centrally		
7.8	The proposed solution shall collect the events occurring on endpoints. The solution shall also provide the functionality to forward of these events to the SIEM.		
7.9	The proposed solution shall provide alerts to users in case of any security incident along with a course of action, in case of any failure to clean		
7.10	The proposed solution must provide notifications for important events. The notifications must be send through email or SNMP traps		
7.11	The proposed solution shall support multiple administrator accounts. Each administrator account shall be configurable with the desired level of management privileges for different components		
7.12	The proposed solution should be capable of providing detailed reports containing data from all the deployed components		
7.13	The proposed solution should allow exporting of reports to PDF or CSV formats		



8	Endpoint Detection & Response		
8.1	The proposed solution should provide contextaware endpoint investigation and response (EDR), recording and detailed reporting of system-level activities to allow threat analysts to rapidly assess the nature and extent of an attack. Custom detection, intelligence, and controls		
8.2	The proposed solution should perform multi-level sweep across endpoints using rich-search criteria as mentioned below		
8.3	User-defined criteria like User Name, File - Name, File – Hash, IP address, Hostname, Registry Key, Registry Value Name & Registry Value Data		
8.4	The proposed solution should be able to create multi-stage detailed kill-chain for performing the root cause analysis of an incident. Cyber Kill chain also provide reputation of the files from the global threat intelligence as well		
8.5	The proposed solution should provide option to sweep and assess the current (point in time/Live) state of the devices.		
8.5.1	1. Scan disk Files		
8.5.2	2. Scan in memory process		
#	Particulars	Bidder's Compliance (Yes/No)	Remarks
8.5.3	3. Search registry		
8.6	The proposed solution to provide the advance response capabilities as mentioned below		
8.6.1	1. Kill process		
8.6.2	2. Isolate device		
8.6.3	3. Block process		
8.7	The proposed solution shall allow ingestion of IOCs (Indicators of compromise) like domains, file-hashes and shall also allow blocking of the files/filehashes/domains/URLs identified by the IOCs		
8.8	The proposed solution should provide contextaware endpoint investigation and response (EDR), recording and detailed reporting of system-level activities to allow threat analysts to rapidly assess the nature and extent of an attack. Custom detection, intelligence, and controls		
8.9	Solution must continuously monitor and report findings as quickly as possible. If an endpoint cannot immediately report findings, results must be stored locally until they can be uploaded to the solution's central management system		



8.10	Solution must provide a way to isolate a system that ensures preventative controls are preserved through reboots. Isolation settings must be preset to allow endpoint to be isolated from threats but able to connect to investigation/remediation systems		
------	--	--	--

EMS

#	Particulars	Bidder's Compliance (Yes/No)	Remarks
	General		
1	The proposed solution should be capable of network lifecycle management, which includes continual discovery of the TCP/IP network, topology mapping, monitoring of all critical network devices for fault and performance, event management - including filtering, correlation, and root cause analysis to ensure compliance with policies.		
2	Collect data from different SNMP devices.		
3	Bidder should propose tools for pro-active automated monitoring and management for inscope IT infrastructure. At a minimum the software should have the following modules:		

#	Particulars	Bidder's Compliance (Yes/No)	Remarks
4	Configuration Management - Should allow the operator to verify and modify the configuration of managed devices-Configuration management tools need to be provided for managing the IT infrastructure at the DC, DR, Near Site, and Head Office. End user devices are out of scope		
	Server Management		
5	The solution should be capable of managing business service events by exploiting agent/agentless data sources and be able to do automatic provisioning of management policies and monitoring templates which are parameterized to specific CI instances in an automatically discovered run time service model with an additional provision to integrate with 3rd party CMDBs and also provide a self-service portal for administrators		



6	The solution should be capable of doing automatic deployment, activation and decommissioning of management policies and monitoring templates based on IT environment changes by performing monitoring audits based on the out of the box topology based event correlation and can report the same, simplifying the IT administrators job.		
7	The solution should have borderless collection of any data from any device in any format from log-generating sources and provide long-term retention of logs and events through high compression ratios with search capability		
8	The solution should support automated enforcement of policies on servers through fully automated check and remediation process. Solution should enable patch policy creation and flexible patch deployments and Supports native patch formats for all major operating systems.		
9	The solution should leverage common event format that does not require familiarity with sourcespecific log formats—thereby avoiding the need for device-or vendor-specific analysis or knowledge.		
	Network Management		
10	The solution should allow for discovery to be run on a continuous basis which tracks dynamic changes near real-time; in order to keep the topology always up to date. This discovery should run at a low overhead, incrementally discovering devices and interfaces		
11	The topology of the entire Network should be available in a single map along with a Network state poller with aggressive/customizable polling intervals		

#	Particulars	Bidder's Compliance (Yes/No)	Remarks
12	Should be able to generate a graphical representation of network. Identify which devices are inactive or out of compliance. Use filters to immediately view isolated specific network segments. Capture a snapshot of the current state of the network, including topology and virtual LAN (VLAN) information. Identify the hosts connected to specific switches or interfaces by MAC address		
13	Deploy and monitor operating system images from a centralized network management system		
	Storage Management		



14	Should provide a simple to use single management interface to understand, control, plan, and manage infrastructure, automatically discover and map the storage network topology and pictorially display objects, paths and zones between an application and the LUN on which the corresponding data resides.		
15	Should provide information on end-to-end capacity reports, graphs, trends, alerts, and policies that are needed to prevent space shortages from impacting your business. It should also help to find orphaned storage that could be utilized to defer unnecessary capital expenditures, and it gives you the data to accurately plan and justify new storage purchases		
16	Should support End to End path provisioning by auto filtering to reduce the amount of time to provision SAN to business application		
	Fault Management		
17	Should provide a Unified Fault, Availability and Performance function from a single station only to reduce network and device loads with unified fault & performance polling for network devices		
18	Topology based and event stream based correlation should be made available to identify faults		
	Asset Management		
19	It should provide a built-in workflow to suggest to the software asset managers in user organization that they should request more licenses or remove installed software that is not in use or assign rights to others users rather than procuring more licenses		
20	It should provide Software Compliance, Contract Management and Financial Charge back capabilities that go beyond asset tracking and provide complete Asset lifecycle management; that provide a real Return On Investment for IT organizations		
21	Proposed solution should have the auto-discovery tool, which should have tight Integration with the proposed ITAM (IT Asset Management) solution.		
	Web infrastructure Management		

#	Particulars	Bidder's Compliance (Yes/No)	Remarks
---	-------------	------------------------------	---------



22	The proposed solution should have the capability to monitor both user and system initiated network traffic between client machines and servers and between servers, collecting network and server performance and availability data in real time, thus enabling administrators to pinpoint the cause of delays and quantify the business impact of detected performance issues related to end users		
	SLA management & monitoring		
23	Solution should be able to report in the context of the business services that the infrastructure elements support—clearly showing how the infrastructure impacts business service levels		
24	Solution should allow to configure downtime for Configuration Items and view the configured downtime in the reports		
25	Collection of performance data should average no more than 3%-5% system overhead		
26	Centralized reporting / MIS for all the modules suggested		
27	Communication between management server and the agent should be encrypted and secured		
28	Effective utilization of bandwidth by selective reporting options		
29	Support to manage all types of operating system through one software		
30	Dynamic Monitoring configuration		
31	Support for backup and storage		
32	Vendor should provide the latest version of the product along with all the latest service packs.		
33	The modules/products should be from a single product family/suite so as to ensure the integration and high level of data exchange between various layers.		
34	It should have an object-oriented, open, and extensible set of common services. These common services should offer a rich and comprehensive set of robust management functions such as event management, Calendaring, communications and administrative function		
35	It should offer Event management as an integral part of the solution. Events should be color-coded on the GUI based on severity		



36	It should also provide an event correlation engine, which should be rules-based and work in conjunction with event management. It should assist in root cause determination and help prevent flooding of non- relevant console messages		
----	---	--	--

#	Particulars	Bidder's Compliance (Yes/No)	Remarks
37	It should be able to provide centralized management of the resources as well as decentralized management through multiple consoles with centralized escalation, reporting and control. Consoles should be able to handle event management as well as provide detailed visualization, association browser / hyperbolic views, progressive/drill down views.		
38	It should provide views to monitor IT resources as business processes. It should provide customizable views, which would reflect business process and allow administrators and operators to monitor the health of the entire business process via one object in the status map		
39	It should have a multi-level, hyper-tier, and scalable manager/agent architecture with multiple lightweight intelligent agents, which allows balancing of the load on the network as well as on the end resources. The manager/agent technology should use the most widely accepted standards, such as SNMP, TCP/IP and UDP		
40	It should have a common object repository based on open standard RDBMS and intelligent information infrastructure, which would allow for transparent access to information repositories and provide data providers for data access		
41	The EMS Solution should be modular and should not be framework dependent so that required modules can be added in future to meet the growing /changing needs		
42	The products provided under EMS, should integrate for providing holistic management of Infrastructure components supporting business		
43	Utilizes a Common Object Repository (COrE) or equivalent feature that allows various modules to share management data		
44	Capability of integrating with third party element manager		



45	Capability to automatically raise trouble tickets to a help desk utility		
46	It should support automatic base lining on historical data, and thresholds that can be adjusted as required, based on data collected		
47	The product should provide full-fledged Service Level monitoring and reporting capability using which administrator should be able to define metrics to be measured, measure on such metrics and do comprehensive service monitoring and webbased reporting based on service availability, downtime and response		

#	Particulars	Bidder's Compliance (Yes/No)	Remarks
48	The tool should be able to measure and collect data from, and set service level reporting on ICMP echo (ping), SNMP MIB variable, services like HTTP, if required. Alerts should be available when the SLA is violated		
49	Should provide Service level management capabilities with detailed reports on the availability, uptime, downtime and outage information status of leased line interfaces, and critical servers		
50	The product should be able to measure, collect, and import performance and SLA data from a wide range of sources, including performance Management modules		
51	It should have a Java Enabled WEB / HTML Based user Interface through which Administrator can access all administrative tasks and operational status monitoring. Similarly it should produce a WEB based interface to the users also for accessing the SLA reports etc.		
52	The product should automatically generate service reports in batch mode and should have capability to upload the reports automatically to a remote web server		
53	The product should also be able to manage metrics using an advanced visualization and analyzing tool for service management metrics. It should be able to display and correlate any combination of metrics in two or three dimensions, which should provide insights into service bottlenecks as well as useful information to aid capacity planning		



54	The product should be scalable. It should support data collectors distributed across locations on collect systems, which should be able to gather and measure statistics from the IT infrastructure if required. Distributed data collection and measurement		
55	The tool should be able to raise performance alerts before peak load conditions are hit		
56	Any performance baselines used by the tool to raise pro-active alerts should be maintained automatically without any recurring manual intervention from application operators		
57	Application alerts raised by the tool should carry actionable information such as the suspect KPI or problem layer (Web, App, or DB).		
58	The tool should have the ability to provide infrastructure capacity utilization trending reports to help plan for growth or de-growth in expected business transaction load on the application		
	Helpdesk Tool		

#	Particulars	Bidder's Compliance (Yes/No)	Remarks
59	The proposed ITIL-based Helpdesk Management System must provide the following features:		
60	The proposed Helpdesk solution should allow a web based GUI ticketing logging system to all the users of OICL to raise self-tickets by them		
61	The proposed solution should provide flexibility of logging, viewing, updating and closing incidents manually via web interface.		
62	The proposed solution should be possible to associate each incident with multiple activity logs entries via manual update or automatically update from other tools or system management tools.		
63	The proposed solution should be able to provide flexibility of incident assignment based on the workload, category, or location.		
64	Each escalation policy should allow easy definition on multiple escalation levels and notification to different personnel via window GUI/console with no or minimum programming.		
65	The escalation policy should allow flexibility of associating with different criteria like device/asset/system, category of incident, priority level, organization and contact.		



66	The proposed solution must provide web-based knowledge database to store useful history incident resolution.		
67	The knowledge tools should provide access on different knowledge articles for different users.		
68	The proposed solution should provide built-in reporting functionality		
69	The proposed solution should allow creation of surveys that allows systematic collection and analysis of customer feedback about service desk performance		
70	The proposed solution should integrate with EMS event management and support automatic problem registration, based on predefined policies.		
71	The proposed solution should be able to log and escalate user interactions and requests		
72	The proposed solution should provide status of registered calls to end-users over email and through web.		
73	The proposed solution should have an updateable knowledge base for technical analysis and further help end-users to search solutions for previously solved issues.		
74	The proposed solution should have the ability to track work history of calls to facilitate troubleshooting.		

#	Particulars	Bidder's Compliance (Yes/No)	Remarks
75	The proposed solution should support tracking of SLA (service level agreements) for call requests within the help desk through service types.		
76	The proposed solution should support request management, problem management, configuration management and change management.		
77	The proposed solution should be capable of assigning call requests to technical staff manually as well as automatically based on predefined rules, and should support notification and escalation over email, web etc.		
78	The proposed solution should provide Knowledge tools as an integral part of Service Desk and these tools should be accessible from the same login window.		



79	It should also have a graphical workflow designer with drag & drop feature for workflow creation and updation		
80	The proposed solution should provide seamless integration to log incident automatically via system and network management.		
81	The proposed solution should integrate with EMS event management and support automatic problem registration, based on predefined policies.		
82	The proposed solution should support request management, problem management, configuration management and change order management.		
83	The proposed ITIL-based Helpdesk Management System must provide the following features:		
84	The proposed ITIL-based Helpdesk Management System must discover incident trends based on analysis of unstructured data. Actionable and fast - problem resolution based on unstructured data from all Service Manager processes. It should displays impact of potential problems based on cluster size of related incidents and determine patterns in thousands of incidents for faster problem isolation		
85	Ability to be kicked off in a self-healing or automatic mode from incidents and provide help to manage closed loop incident management process in case of monitoring events		
86	Should create automated IT process workflows for closed loop change and incident management. User should be given options to execute workflows in one of three modes: automated, visually guided or operator initiated, and prescheduled.		

#	Particulars	Bidder's Compliance (Yes/No)	Remarks
87	Should provide a web-based management dashboard for visibility into ITIL incident management and problem management data. Includes out-of-the-box reports, such as MTTR trending, cumulative return on investment (ROI), most frequent resolution workflow, and incident and alert trending correlated to ITIL configuration items. Users should be allowed to create custom reports.		
	Security & Patch Management		



88	Proposed solution should do granular filtering of software patches based on environment requirements		
89	Proposed solution should schedule, deliver and track operating system and automate patch delivery		
90	Proposed solution should provide industry recognized patch management and distribution mechanism		
91	Proposed solution should provide automated OS and application patch management		
92	Proposed solution should remedy vulnerabilities and enforce security policies		
93	Proposed solution should schedule periodic scans of computers to identify missing patches		
94	Proposed solution should identify and download missing patches from vendors' websites		
95	Proposed solution should download required patches and create tasks to schedule patch deployments		
96	Proposed solution should be supported for deployment of patches on all in scope components		
97	Proposed solution should have bundled reporting software so no third party tools would be required to customize reports		
98	Proposed solution should be able to provide audit reports		
99	Proposed solution should be capable of integrating with one or more Active Directory structures whenever required		
100	Proposed solution should be capable of using existing client computers as distribution points at remote sites without the need of allocating dedicated servers		
101	Proposed solution should be able to install package through following mechanisms: Push Pull User self-service		

#	Particulars	Bidder's Compliance (Yes/No)	Remarks
102	Proposed solution should have the ability to throttle bandwidth, either statically or dynamically. The throttling capability must support up and down stream throttling for both the server and agents		



103	Proposed solution should be able to deploy agents using IP address/hostname and port to the agent deployment, the patches can be deployed		
104	Proposed solution should support centralized architecture		
105	Proposed solution should support virtualized environment too		
106	Proposed solution should provide remote agent deployment utility for installing agents remotely. The tool should be able to use Active Directory or Local Administrator Authentication for deploying agents to remote computers		
107	Proposed solution should provide easy to use in-place upgrade procedures for all components through the console		
108	Proposed solution should have native support for high level of encrypted communications without any dependency on additional software, hardware, third party certificates or Certificate Authority		
109	Proposed solution should have the ability to do centralized patch management for PCs, Laptops, Servers		
110	Proposed solution should support the IPv4 & IPv6		
111	Proposed solution should support centralized administration, role based access control and administration without much load on the network		
112	Latest fixes/ updates should automatically be downloaded to the patch management server as per the policies/ schedule for patch download once the patch is made available on software vendor's website.		
113	If any information or payload (e.g. Patch Metadata or Patch binaries) is downloaded from internet, then the integrity of all such content must be verified by the proposed solution using checksums to ensure that the content downloaded has not been modified or corrupted. File checksums and file sizes must be compared to make sure that the downloaded file is intact and unchanged		
114	Proposed solution should be able to determine if a patch has already been installed on a node, even though it is assigned manually. Proposed solution should have the capability to analyze appropriate patches of the OS/ applications for the Desktop/ server in comparison to the latest available patches/ updates released by respective OEMs		



#	Particulars	Bidder's Compliance (Yes/No)	Remarks
115	Proposed solution should be able to detect the required patches according to individual node's configuration		
116	Proposed solution should allow users to postpone the deployment of a patch for a period of time determined by the administrator		
117	Proposed solution should support event-driven remediation.		
118	Proposed solution should support rollback of patches and service packs applied, if rollback is supported for that particular Patch/Service packs		
119	Proposed solution should have the capability for remediation i.e. continuously deploy, monitor, detect and enforce patch management policies		
120	Proposed solution should be able to deploy any software/ files through the patch management solution		
121	Proposed solution should have the capability to generate report specific to one group of servers/endpoints or should be capable of generating reports with an enterprise view		
122	Proposed solution should be able to verify if the patches on desktop are correctly installed by confirming that the vulnerability has been remediated		
123	Proposed solution should come along with standard reports and should generate customized reports as per business requirement		
124	Proposed solution should support various reporting formats i.e. reports can be downloaded easily and or exported		
125	The Proposed Solution should have the ability to consolidate data and to produce a single report for inscope Clients/Endpoints		
126	Proposed solution should support regulatory specific reports		
127	Proposed solution should be able to manually group computers together for deployment of patches. Proposed solution should provide the ability to dynamically group computers based on asset and software information		
128	Proposed solution should support the grouping of patches into a 'baseline' which can take the form of monthly patch bundle e.g. 'Critical Patches'		



129	Proposed solution should be able to re-deploy the patch on a computer automatically if the initial deployment is not successful and even if the deployed patch is un-installed by the user		
-----	--	--	--

#	Particulars	Bidder's Compliance (Yes/No)	Remarks
130	Proposed solution should support granular control over re-boot process after patch deployment like prompting user, allowing user to differ, rebooting immediately if no one has logged on, etc.		
131	Proposed solution should come along with all operational technical manuals along with other related documents		
132	Proposed solution should be able to identify the computers that have installed the patch that is to be rolled back on need basis		
133	Proposed solution should be able to provide realtime (within minutes) patch deployment status monitoring		
134	Proposed solution should allow console operator to deploy patches to all computers via a central console without intervention from the users or allow console operator to target which computers to deploy the patches to		
135	Proposed solution should allow console operators to spread the patch deployment over a pre-defined period of time to reduce overall impact to network bandwidth		
136	Proposed solution should be capable of generating reports on patches deployed, when, by whom, to which endpoints, etc.)		
137	Proposed solution should be able to identify systems with non-patched vulnerability conditions		
138	Proposed solution should allow the console user to deploy actions to remediate against the vulnerabilities identified		
139	Proposed solution should have the dashboard to drill down to show details for both compliant and non-compliant systems, including but not limited to, non-compliant controls, component name, category, identifier and type		
140	In the proposed solution, information reported should not be more than 1-7 days old for devices that are active on the network		



141	The reporting module should contain, but not limited to, the following reports: (i) Progress of all patches applied (ii) Patch Compliance report for selected month /System (iii) Monthly Patch Compliance report for single patch (iv) Total number of computers managed and the distribution of these computers;		
142	Proposed solution should allow console operators to export report in CSV, PDF, XLS & HTML format		

#	Particulars	Bidder's Compliance (Yes/No)	Remarks
143	Proposed solution should allow console operators to customize and save the reports without the use of third party reporting tools		
144	Proposed solution should allow console operators to drill-down from the report to the specific computers		
145	Proposed solution should allow console operator to trigger alerts when user-defined conditions are met		
146	Proposed solution should generate both prepackaged and custom, wizard generated reports like compliance reports can be generated for one month patches or one particular patch on all system or on one system		
147	Proposed solution should be capable of software distribution and installation e.g. Chrome patches, MS Office patches		
148	Proposed solution should have automatic patch management and deploy patches for various platforms including Windows, Linux/Unix, Solaris and AIX		
	Reporting and Dashboards		
149	In the proposed solution reports should be scheduled to be run and sent to administrators at specified times and intervals		
150	In the proposed solution, reports should be viewed online		
151	In the proposed solution, reports should be downloaded in CSV, PDF, TXT and XML formats		
152	In the proposed solution, reports should be sent through emails		
	AI and Intelligent Virtual Agents		



153	Use of Machine Learning/Artificial Intelligence/Speech to Text /Natural language Understanding in IVA Transactional Capability		
154	Deployment Option On-Premise / Cloud		
155	Integration with Telephony / IVR platform for voice enabled human voice conversations		
156	Options to send Customer links with Virtual Agent Guidance for uploading Issue related Images		
157	Capability to integrate with ITSM tools and Digital Channels like IVR, Webchat, What's app, Agent screens, backend systems like CRM using APIs, Web Services. Custom Adapters etc		
158	Text to speech and speech to text conversion and NLP Engine		
159	Multi Language Support, integration with translation services		
160	Micro service architecture and Scalability for enhanced add-on Services.		
#	Particulars	Bidder's Compliance (Yes/No)	Remarks
161	Industry Compliance and Security Capabilities like AES256 encryption, data privacy, SAML/SSO, multi factor authentication		
162	Post deployment ready to provide skilled manpower for proactive monitoring, technical and functional support.		
163	Ability to handle the exceptions based on the business rule such as frustration based, intent based, scheduled when the chatbot is unable to process request after specified attempts etc.		
164	Sentimental Analysis and Service Level Analytics		
165	Agent Screen Option		
166	Agent assist / Knowledge Based search		
167	Platform option for OICL administrator for Training the BOT		
168	UI based interface to create new flows as per UIIC requirements		
169	Easy to use Widgets for Location, Flow creation, Input options, voice / text options		
170	AI based ITSM solution should have the capability to interface with ITSM tools, RPA or any other systems as applicable. (Webhook, File upload, API etc.)		
171	Options to Integrate with video call and Co browsing for remote support		



Helpdesk Solution

#	Particulars	Bidder's Compliance (Yes/No)	Remarks
1	ITIL certification		
1.1	The proposed IT Service Management solution should be built on ITIL framework and must be officially certified on the current ITIL v4 best practices on at least 10 processes by Pink Elephant. The ITIL4 processes that are relevant and needs to be assessed to meet the minimum functional criteria are Incident management, Problem Management, Change Enablement, Service Configuration management, Service Catalog Management, Release Management, Service Desk, Knowledge Management, IT Asset Management and Service Request Management. The certification copy to be submitted along with the formal technical response.		
1.2	It should provide built-in reference process templates for Incident/Service requests/problem and change management.		
2	Web based interface		
2.1	Service desk should provide web-based interface and should not require any client software to be		

#	Particulars	Bidder's Compliance (Yes/No)	Remarks
	installed.		
2.2	All users in the organization should have a provision to log the call directly and view the progress.		
2.3	Users should have an option to accept or reject the resolution provided by the helpdesk team and solution should also have the survey mechanism to get the user feedback.		
3	Service desk module should provide detailed user management functionality including		
3.1	Single sign of support and ability to interface with LDAP		
3.2	Automatic sync-up with LDAP server		
3.3	Role based access control		
3.4	Ability to create roles based on the business need		
3.5	Standalone user authentication algorithm, If the LDAP server is not available		



4	Workflow support / State machine		
4.1	Ability to define states which shall be part of the work-flow		
4.2	Should provide out-of-the-box categorization, as well as routing and escalation workflows that can be triggered based on criteria such as SLA, impact, urgency, CI, location, or customer.		
5	Forms / Custom fields		
5.1	System should provide facility to display different forms/templates for input gathering based on the nature of service-request/incident.		
5.2	Service requests pages may require custom fields for accepting inputs as part of service-request submission or during any state transition. System should allow the definition of such custom fields and link it against the service-request work-flow		
5.3	There should not be any restrictions on the number of custom fields which can be defined.		
5.4	Custom fields should be based on HTML controls like Date-time, Numeric, Text, Grid controls, etc. System should also support generating forms based on the collected data for auditing purpose (ex: service request form for internet access etc.,)		
5.5	Should support validation rules on the custom fields		
5.6	Access control restriction should be supported on the custom fields (user/role based)		
6	The support person can interact with the end users through chat in built and add those chat transcripts in the ticket.		
7	Service request submission		



#	Particulars	Bidder's Compliance (Yes/No)	Remarks
7.1	System should allow flexible submission of service requests. Helpdesk engineer should be able to log calls on behalf of the callers		
7.2	System should allow web based call logging		
7.3	System should allow automatic conversion of email to service requests		
7.4	Upon submission, every request should be assigned with unique-id which shall remain unique throughout the lifecycle and the request id should not be re-used. It should be possible to customize the numbering format of the generated request (ex: date-month-branch ID - type of asset - xxx)		
8	Engineer Availability / Attendance tracking		
8.1	System should provide a facility to track engineer's attendance and availability for taking up the call.		
8.2	Helpdesk should have a facility to check the availability of engineer(online) before assigning a call to avoid SLA breaches.		
9	Service request management		
9.1	Helpdesk engineers should be able to assign the service request to field persons and track it to closure.		
9.2	System should provide integrated approval mechanism for getting approval from higher authorities upon a need. Flexibility to be provided to route the approvals automatically without the need of helpdesk/human intervention. Should provide approval managers an option to set 'delegation' in case they are unavailable for a period of time		
10	Attachment support		
10.1	System should support the possibility of attaching scanned copies, documents, etc. as part of request submission. Ability to configure the permitted file extensions and file limits should be supported		
10.2	There should not be any limits on the number or the size of the attachments supported		
11	Business Rules / Actions Support		
11.1	System should support the possibility of triggering custom actions upon any state transitions in the request lifecycle		



11.2	System should support actions before and after the state transitions		
12	E-mail / SMS Notifications		
12.1	System should support notifying the users via SMS or E-mail		
12.2	The system should provide flexibility to configure when the SMS or E-mail should be sent		

#	Particulars	Bidder's Compliance (Yes/No)	Remarks
12.c	The contents of E-mail should be configurable including the selection of request-fields which should be part of the mail body		
13	Automatic assignment / State transition		
13.1	System should provide flexibility to assign the requests to the field engineers automatically		
13.2	System should support automated state transition based on the configuration. i.e. If the approval has been performed by the approval manager, it should automatically move to next state without the need for manual intervention		
13.3	The state transitions shall also be automatic based on an email response.		
14	Functional & Hierarchical Escalation		
14.1	System should provide a mechanism for achieving functional escalation & hierarchical escalations		
14.2	This should be granular and should support the flexibility to configure at a specific functional unit level (desktop, network, server, application, etc.)		
15	Knowledge base		
15.1	System should provide an ability to create and maintain the knowledge base		
15.2	Knowledge base should provide options like private and public where in public is visible to every-one and private is visible only to the service engineers		
15.3	Knowledge base articles should be approved by the knowledge base administrators		
15.4	Ability to the users in the system to rate/survey the usefulness of the Knowledge Base articles		
15.5	Knowledge Base articles to be automatically popped up to the users in the system whenever it is relevant to the ticket that is logged		
16	Operational Level Agreement (OLA)		



16.1	System should provide an ability to define operational level agreement where-in operational level agreements between the inter department can be tracked		
16.2	OLA tracking should provide escalation mechanism (prior and post violation) and any such escalation should support SMS and E-mail		
16.3	It should be possible to define OLA based on any service request fields (i.e. including custom fields)		
16.4	Should support business hours and non-business hours based OLA definition and measurement		
16.5	Service request should keep the details of transactions and provide granular details about the violation, where it occurred, etc.		
17	Service Level Agreement (SLA)		

#	Particulars	Bidder's Compliance (Yes/No)	Remarks
17.1	System should provide an ability to define Service level agreement where operational level agreements can be tracked.		
17.2	SLA tracking should provide multiple levels of escalation mechanism (prior and post violation) and any such escalation should support SMS and E-mail		
17.3	System should support pre-violation notification capability to alert the helpdesk users and operators before the violation occurs		
17.4	It should be possible to define SLA based on any service request fields (i.e. including custom fields)		
17.5	Should support business hours and non-business hours based SLA definition and measurement		
17.6	Service request should keep the details of transactions and provide granular details about the violation, where it occurred, etc.		
17.7	It should be possible to calculate the penalty for SLA violations		
18	Feedback / Survey		
18.1	System should provide an ability to capture user feedback on the resolution and be able to generate reports based on the same.		
18.2	Generic survey module should be provided which should help the organization to conduct survey among the selected users.		



18.3	The questions and response options should be completely configurable		
19	Business Hours & Holiday profile		
19.1	System should provide an ability to define multiple business hours and holiday profiles which should be applied automatically for SLA and OLA calculation		
19.2	Business hour definition should be flexible to define 6 days, etc. Also, system should be able to provision for lunch break, etc. as part of business hour definition		
20	User Access Control - System should support separate user access control for service-desk. Each of modules like service request fulfilment, Incident, etc. should support separate user-access control. Using this, it should be possible to specify who shall have an access to which modules.		
21	Service desk shall be accessible from smart-phone browsers and shall provide mobile device friendly interfaces.		
22	The Service desk shall be accessible with different views:		
	a. Real-time help-desk Console view		
	b. Reporting view for executives		
23	Real-time helpdesk Console requirements:		

#	Particulars	Bidder's Compliance (Yes/No)	Remarks
23.1	Shall be a single real-time console accessible via a web browser that Provides an end-to-end status of all request status view by hour, day, week, month, and year.		
23.2	Shall be able to configure the custom dashboards based for the different users and it should appear upon login		
24	Reporting Requirements		
24.1	Shall include a tool for generate asset and inventory reports based on the available data		
24.2	Shall also provide for a tool which analyses collected data with a variety of different reporting functions.		
24.3	Shall be able to filter report data by transaction, by specific monitored location and user-defined regions.		



24.4	Shall allow end-users to browse all reports using Internet Explorer without the need to install additional report viewing software.		
24.5	When viewed in a web browser, shall allow flexibility to		
	1. Save reports as XLS/PDF		
	2. Email the reports/view that is currently viewed		
24.6	Shall be able to automatically generate daily reports and automatically sent by email at a pre-defined schedule to any recipient.		
24.7	Shall provide custom report manager for generating custom, personal reports. The custom reports can be viewed online or scheduled for sending via email directly to designated recipients.		
25	Security requirements:		
25.1	All sensitive data (passwords etc.) should be encrypted in the system.		
25.2	The overall end-to-end helpdesk solution shall be secured.		
25.3	The servers shall allow multilevel authorization for administrators controlled using custom defined roles		
26	Availability requirement - The total solution shall avoid any single point of failure. A failure at any point shall not affect any services at any time		
27	Ease of Provisioning and Troubleshooting Requirements:		
27.1	The solution offered shall provide ease of use in provisioning, maintenance and troubleshooting. Preferably by a command console interface as well as a graphical user interface shall be provided so that changes can be made in-band as well as out-ofband.		
27.2	Dynamic configuration changes shall be possible without having to reboot the box.		

#	Particulars	Bidder's Compliance (Yes/No)	Remarks
27.3	It shall be possible to upgrade configuration files and operating system images over the network without requiring a person to physically be present at the site.		



28	E-mail Integration - System must provide an option to integrate with E-mail server (POP3, IMAP, SMTP) for sending and receiving e-mails.		
29	Help Desk for Other business Applications		
29.1	Help Desk module must be easily configurable to handle support operations of other OICL business applications like HRMS, Web Portal Application, etc. For these business applications, separate response & resolution teams shall be involved. Only that team shall have an access to view and work on the calls. Rest of the teams including IT must be a user for such Projects/Processes.		
29.2	For these requirements, the solution must facilitate virtual service desk instance approach. It cannot be a service in the primary incident management or Service request management system.		
30	Solution should support multi-tenancy with complete data isolation as well as with ability for analysts based on access rights to view data for one, two or more organizational units.		
31	The support person can interact with the end users through chat in built and add those chat transcripts in the ticket.		
32	A virtual bot should be available, which can respond to user requests, immediate via portal, email or mobile interfaces.		
33	The support person can interact with the end users through chat in built and add those chat transcripts in the ticket.		
34	Beyond mobile iOS and Android apps, Self Service App should be available on any device with an HTML5 browser.		
35	The tool should allow the user to take a screenshot of the error message and sends it to the service desk. The user can type in a couple of text lines to describe the error in simple language. The service desk agent then can pick up the ticket with the information already filled in (category, impact, and assignment).		
36	Should provide modern data analysis methods for insight and value to service desk by leveraging unstructured as well as structured data.		
37	The solution should provide to browse through CMDB which should offer powerful search capabilities for configuration items and services, enabling to quickly find CIs as well as their relationships to other CIs.		



#	Particulars	Bidder's Compliance (Yes/No)	Remarks
38	The solution should have a single CMDB across ITSM and Asset Management system.		
39	The proposed Asset Management solution should evolve on a common, expandable platform - IT Service Management, Asset Management, Software Asset Management, AIOps.		
40	The proposed Asset Management solution should understand how each assets delivers IT services and business applications in today's multi-tiered architectures.		
41	The proposed Asset Management solution should consolidate, end-to-end lifecycle management of IT hardware and software assets.		
42	The proposed Asset Management solution should easily request and fulfil assets from approved vendors through procurement workflows and selfservice catalogue.		
43	The proposed Asset Management solution should control asset costs with financial management.		
44	The proposed Asset Management solution should provide Software Asset Management Compliance Dashboards.		
45	The proposed Asset Management solution should provide License Reconciliation feature like Automated reconciliation of licenses between versions based on utilization delivers a software version matrix so you can easily upgrade or downgrade licenses.		
46	The proposed Asset Management solution should provide Service Asset & Configuration Management feature, but not limited to:		
46.1	Manage the business better through dashboards that provide a quick overview of various kinds of assets, allowing you to understand, organize, and track assets effectively.		
46.2	Efficiently track and manage assets through life cycle with out-of-the-box workflows. Customize rules to manage workflows based on business needs.		
46.3	Understand and manage assets and CI topologies by creating relationships between devices and service components, system element records, infrastructure, and peripheral assets.		



47	The proposed Asset Management solution should provide Software Asset Management feature, but not limited to:		
47.1	Built-in smart dashboards and compliance tools		
47.2	Avoid software audit risks and associated costs		
47.3	Vendor specific predefined license rules and metrics		
47.4	Optimal utilization of licenses		

#	Particulars	Bidder's Compliance (Yes/No)	Remarks
47.5	Automated license reallocation		
47.6	Software asset management optimization		
47.7	Vendor audits risk avoidance		
47.8	Compliance management through dashboards and reporting		
48	The proposed Software Asset Management solution should be able to do following:		
48.1	Monitor consumption: Enjoy vendor-specific, out-of-the-box license rules and metrics to accurately track software consumption.		
48.2	Optimize license usage: Upgrade or downgrade licenses to optimally utilize licenses based on consumption or utilization.		
48.3	Ensure compliance: Use out-of-the-box dashboards to easily view and manage compliance status for OnPrem and SaaS deployments.		
48.4	Track software spend: Track organizational spend on software for better financial management and budget rationalizations.		
49	The proposed Asset Management solution should have hardware, portfolio, contract, vendor, procurement, and financial management– all included.		
50	The proposed Asset Management solution should have natively built-in CMDB and IT discovery as single OEM solution.		
51	The proposed Asset Management solution should provide flexible licensing: named and concurrent users.		
Asset Discovery Specifications			
1	Discovery should work without requiring agent installation (that is, agent-less discovery) while discovery Layers 2 through Layers 7 of OSI model.		



2	Should use Industry-standard protocols such as WMI, SNMP, JMX, SSH to perform discovery without requiring the installation of an agent.		
3	Discovery system should have the ability to capture configuration files for the purposes of comparison and change tracking.		
4	Discovery system should be capable of supporting role-based access to various aspects of CMDB administration.		
5	Discovery should be object-oriented, allowing specific CIs and relationships to be discovered using a library of discovery patterns.		
6	Discovery engine should gather detailed asset and configuration item (CI) information for specific servers and the applications running on them.		
7	Solution should dynamically discover and continuously map IT hardware inventory and		
#	Particulars	Bidder's Compliance (Yes/No)	Remarks
	service dependencies.		
8	Discovery system should have ability to modify outof-box discovery scripts, create customized discovery scripts.		
9	Discovery system should have ability of container discovery (Docker, Kubernetes, OpenShift).		
10	Solution should provide a portal to search Configuration Items using natural language understanding.		
11	Proposed Tool should support discovery of VMware storage topology including VMware data stores, VM file systems, local storage on the ESX servers and the relations between them.		
12	Proposed Tool must support storage elements discovery, including storage arrays, logical disks, and interconnectivity between SAN elements.		
13	Proposed Tool must support, system Center Virtual Machine Manager (SCVMM) Discovery and VMware vRealize Operations Manager (vROps) and Red Hat Virtualization Discovery to get infra/hosts details from virtualization platform.		
14	Proposed Tool should be able to provide accurate discovery even with intermittently connected devices, or from behind firewall or VPN.		



15	Solution should maintain the discovery of historical data as well as up to date information and detect the asset changes.		
----	---	--	--

10.2 Appendix 2: Commercial Bill of Material

<Sheet for Bill of Material is attached as a separate file>