The Oriental Insurance Company Limited

Head Office, New Delhi

Request for Proposal

For

Selection of Vendor for Supply, Installation, Implementation, Development & Maintenance of Web Portal and Mobile app

(Tender Reference No.: OICL/HO/ITD/WEBPORTAL/2022/01 Dated 31 May 2022)

Information Technology Department

The Oriental Insurance Company Limited
2nd Floor, Oriental House,
A-25/27, Asaf Ali Road,
New Delhi- 110002

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/WEBPORTAL/2022/01 Dated 31 May 2022**
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**

NEFT Details for Payment of Tender Fees:

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**

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/WEBPORTAL/2022/01 Dated 31 May 2022**
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 © 2020 The Oriental Insurance Company Limited.

Table of Content

1 Introduction 15

1.1 About the Company 15
1.2 Notice Inviting Bids 15
1.3 Project Objective 15
1.4 Schedule of Events 16
1.5 Availability of tender document 17
1.6 Eligibility Criteria 18
1.7 Project Timelines 23

2 Scope of Work 25

2.1 Existing Setup 26
2.1.1 Existing Stakeholders of Portal and Mobile app 26
2.1.1.1 Customers 26
2.1.1.2 Corporate Customer 27
2.1.1.3 Agents / POSP 27
2.1.1.4 Brokers 27
2.1.1.5 Dealers 27
2.1.1.6 TPA (Third Party Administrators) 27
2.1.1.7 Surveyor 27
2.1.1.8 Advocate 27
2.1.1.9 Pensioner 27
2.1.1.10 Employee 28
2.2 Current Scope 28
2.3 Additional Items 29
2.4 Project Phase 29
2.5 Solution Design 30
2.5.1 END to END IT Architecture 30
2.5.2 24X7 Availability 30
2.5.3 Liaison with existing OICL Vendor / OEM's 30
2.5.4 Bilingual 30
2.5.5 Manuals / Documents 31
2.5.6 Integration with existing Applications 31
2.5.7 Projections 32
2.6 Detail Scope of Work 33
2.6.1 Phase I - Requirement gathering and develop the portal and mobile app with all other items 33
2.6.1.1 Requirement gathering 33
2.6.1.2 Development of Portal and Mobile app 34
2.6.1.3 Hosting 40
2.6.1.4 Content & Data Migration 42
2.6.1.5 System Integration testing 44
2.6.1.6 Security 44

2.6.1.7 Data Encryption & Object Signing 45
2.6.1.8 Securing Data at Rest 46
2.6.1.9 Data Integrity 46
2.6.1.10 Load balancer 47
2.6.1.11 Document Management 47
2.6.1.12 Content management 48
2.6.1.13 Integration with Social Media 49
2.6.1.14 Search capabilities and Optimization 49
2.6.1.15 Web Analytics 49
2.6.1.16 Workflow Capability & Profile based functionalities on the fly 50
2.6.1.17 Redesign, Content Presentation 50
2.6.1.18 Mobile Application 50
2.6.1.19 Integration with Payment Gateways 51
2.6.1.20 Openness 52
2.6.1.21 Software vendor neutrality 53
2.6.1.22 Architecture, Auto Scaling & Performance 53
2.6.1.23 Scalability 53
2.6.1.24 Design and development of Intelligent Data Analytics dashboards 54
2.6.1.25 SSL Certificate or any Certificate or security component 54
2.6.1.26 Ticketing Tool 54
2.6.1.27 Phase 2- Underwriting Logic 55
2.6.1.28 Application integration 55
2.6.1.29 Benchmarking 56
2.6.1.30 Encryption, HSM, KSM & Digital Signature 58
2.6.1.31 API gateway 60
2.6.1.32 ADR 61
2.6.1.33 APM 62
2.6.1.34 AI enabled Chat Bot / Voice Bot 64
2.6.1.35 Password Less Authentication 65
2.6.1.36 Audit & Governance Requirements 66
2.6.1.37 Quality Assurance & Audit 66
2.6.1.38 3rd party Audit Certification 67
2.6.1.27 Hardware 68
2.6.1.28 DR Setup 70
2.6.1.29 Software 71
2.6.1.30 External Agency for UAT and Data Migration Audit 71
2.6.1.31 Project Management 75
2.6.1.32 Minimum Resource On-site Deployment during implementation phase 79
2.6.1.33 Training 81
2.6.1.34 Go-Live 82
2.6.2 Phase – 2 - Facilities Management and AMC/ ATS 82
2.6.2.1 Domain Services 82
2.6.2.1.1 Database management 83

2.6.2.1.2 Server Management 87
2.6.2.1.3 Storage Management 93
2.6.2.1.4 Backup and Restoration Management services 95
2.6.2.1.5 DC – DR Drills 98
2.6.2.1.6 RTO / RPO Management 98
2.6.3 Cross Functional Services 99
2.6.3.1 Incident Management and IT Infrastructure Support Services 100
2.6.3.2 Change Management and Release Management: 102
2.6.3.3 Service Level Management 104
2.6.3.4 Security Management: 105
2.6.3.5 Patch Management 110
2.6.3.6 Software License Management: 111
2.6.3.7 IT service continuity and Disaster Recovery 111
2.6.3.8 Application Performance Management 112
2.6.3.9 Roles and Responsibility of APM, ADR, API gateway, Chatbot, password less authentication, HSM and KSM L1, L2 Resources 112
2.6.3.10 Exit Management Services 114
2.6.4 Application Management 117
2.6.4.1 Level One (L1) Support 117
2.6.4.2 Level Two (L2) Support 118
2.6.4.3 Level Three (L3) Support 119
2.6.4.4 Helpdesk Support 120
2.6.5 Minimum Deployment of resources during Sustenance Phase 120
2.6.6 Desired Qualification and Experience of Resources 121
2.6.6 WARRANTY & ON-SITE MAINTENANCE 122
3 Terms & Conditions 126
3.1 General 126
3.1.1 Definitions 126
3.1.2 Amendment to Bid Document 126
3.1.3 Sub-contracts 127
3.1.4 Acceptance of the Solution 128
3.1.5 Conditional bids 128
3.1.6 Submission of Bids 128
3.1.7 Performance Security 129
3.1.8 Pre-Bid Meeting 129
3.1.9 Installation and Implementation 129
3.1.10 Delay in Bidder's performance 129
3.1.11 Payment terms 130
3.1.12 Mode of Payment 132
3.1.13 Penalties and delays in Bidder's performance 132
3.1.14 Currency of Payments 132

3.2 Other RFP Requirements 132
4 Terms of Reference ('ToR') 136
4.1 Contract Commitment 136
4.2 Ownership, Grant and Delivery 136
4.3 Completeness of Project 136
4.4 Compliance 136
4.5 Assignment 137
4.6 Canvassing/Contacting 137
4.7 Indemnity 137
4.8 Inspection of Records 138
4.9 Publicity 138
4.10 Solicitation of Employees 138
4.11 Information Ownership 138
4.12 Sensitive Information 138
4.13 Technological Advancements 139
4.14 Confidentiality 139
4.15 Guarantees 140
4.16 Liquidated Damages 140
4.17 Termination for Default 140
4.18 Force Majeure 140
4.19 Termination for Insolvency 141
4.20 Termination for Convenience 141
4.21 Resolution of disputes 141
4.22 Governing Language 142
4.23 Applicable Law 142
4.24 Prices 142
4.25 Taxes & Duties 142
4.26 Deduction 142
4.27 No Claim Certificate 143
4.28 Cancellation of the contract & compensation 143
4.29 Rights reserved by OICL 143
4.30 Limitation of Liability 144
4.31 Waiver 144
4.32 Violation of terms 144
4.33 Repeat Order 144
4.34 Integrity Pact 144
4.35 Intellectual Property Rights 145
4.36 Outsourcing Agreement 145
4.37 Regulations, Legal & Compliance 146
4.38 Guidelines for MSME 147
4.40 Instruction for Online Bid Submission 148
4.41 Procurement through Local Suppliers (Make in India) 148
5 Instruction to Bidders 150

5.1 Tender Bidding Methodology 150
5.2 Bid Security 150
6 Bid Documents 151
6.1 Eligibility Bid Documents 151
6.2 Technical Bid Documents 151
6.3 Commercial Bid Documents 152
6.4 Mandatory Documents required in Hard Copies (offline) 153
6.5 Eligibility Evaluation 153
6.6 Technical Evaluation 154
6.7 Commercial Evaluation 156
7 Service Level Agreement 158
7.1 System Availability 158
7.2 Issue Criticality Classification 158
7.3 Service Level Default 159
7.4 Penalty Computation 170
7.5 Incident Matrix 170
7.6 AT RISK AMOUNT 171
7.7 Other Conditions 171
7.7.1 Exception 172
8 Disclaimer 173
9 Annexure 174
9.1 Annexure 1: Application form for Eligibility Bid 175
9.2 Annexure 2: No Blacklist Declaration 176
9.3 Annexure 3: Contract Form 177
9.4 Annexure 4: Query Format 179
9.5 Annexure 5: Bid Security Declaration 180
9.6 Annexure 6: Pro forma for Performance Security 182
9.7 Annexure 7: Statement of No Deviation 183
9.8 Annexure 8: Office locations and service infrastructure facilities 184
9.9 Annexure 9: Bidder Profile 185
9.10 Annexure 10: OICL Present IT Setup 186
9.11 Annexure 11: Undertaking of Authenticity for Appliance and Equipment Supplies . 187
9.12 Annexure 12: Manufacturers Authorisation Form 188
9.13 Annexure 13: Non-Disclosure Agreement 189
9.14 Annexure 14: Integrity Pact 194
9.15 Annexure 15: Functional and Technical Specifications 201
9.16 Annexure 16: Bill of Material 202
9.17 Annexure 17: Land Border with India 203
9.18 Annexure 18: Sizing Adequacy Letter 204
9.19 Annexure 19: Project Team Profile (Individual) Detailed 205
9.20 Annexure – 20 Stack Confirmation 207

Purpose of this document

The purpose of this Request for Proposal (hereafter referred to as "RFP") is to define scope of work for the Bidder for Request for Proposal for Selection of Vendor for Supply, Installation, Implementation, development & Maintenance of Web Portal and Mobile app.

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	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
CSP	Cloud Service Provider

MSP	Managed Service provider
SI	System Integrator

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 900+ Business Centers/micro offices geographically spread out across India. Currently head office has 5 buildings located in New Delhi along with OSTC Faridabad.

As on date, all offices of OICL are provisioned with dual active-active links using MPLS over RF, leased lines etc. Further, Roam connectivity is provided to 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 approx 10 million new policies in the year 2019-20. The Company has more than 250 General Insurance products to cater to the varied insurance needs of its customers. It also has a strong workforce of about 12,000 employees and over 35,000 agents. The Company has a web portal www.orientalinsurance.org.in for use of its customers and agents with a provision for premium calculator, payment gateway and online issue/ renewal of policies.

1.2 Notice Inviting Bids

The Deputy General Manager (IT), The Oriental Insurance Company Limited invites online bids from eligible companies / organizations/firms to “Selection of Vendor for Supply, Installation, Implementation, development & Maintenance of Web Portal and Mobile app” to OICL for a period of 5 years.

The selected Bidder is required to familiarize itself with OICL’s environment and infrastructure before the start of the contract.

1.3 Project Objective

The Government of India has paved the way for mass adoption of Cloud services by the Government and Public sector organizations by empaneling the CSPs with Ministry of Electronics & Information Technology (MeitY). MeitY has also empaneled Cloud Service Offerings of private Cloud Service Providers (CSPs) which could be availed by the OICLs under this initiative. The CSPs are empaneled to offer Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) under the three Cloud Deployment models namely, Public Cloud (PC), Virtual Private Cloud (VPC) and

Government Community Cloud (GCC). MeitY vide its document "Guidelines for Enablement of government department for Adoption of Cloud" version 1 has opined that" Cloud enables OICLs to procure tools and technologies which are not feasible and viable to procure as a part of standard IT procurement. OICL should adopt a 'Cloud-by-Default' approach when designing a new IT service/ application or migrating or enhancing an existing application to reap both financial and non-financial benefits of cloud. Any exception to the Guidelines/ Policy shall be with the approval of Department's competent authority. "

The Oriental Insurance Company Ltd. (OICL) being a public sector organization under Ministry of Fnance , Govt. of India accordingly envisages to Select Vendor for Supply, Installation, Implementation, development & Maintenance of Web Portal and Mobile app to be hosted on public cloud based on PaaS/Iaas model of hosting using microservices and containers based architecture and is to be capable of performing fresh policy issuance and renewals (to be setup in a loosely coupled and independent fashion) with real time sync to core insurance database . OICL proposes to invite online bids from eligible Bidders having proven past experience in providing Portal and Mobile app for the same.

1.4 Schedule of Events

General Details	
Department's Name	Information Technology Department
Scope of Work	Selection of Vendor for Selection of Vendor for Supply, Installation, Implementation, development & Maintenance of Web Portal and Mobile app
Tender Details	Request for Proposal for Selection of Vendor for Selection of Vendor for Supply, Installation, Implementation, development & Maintenance of Web Portal and Mobile app
Tender Type	Open
Tender No.	**OICL/HO/ITD/WEBPORTAL/2022/01 Dated 31 May 2022**
Consortium	No
Download Tender Documents	Document to be purchased from Information Technology Department, The Oriental Insurance Company Limited, Asaf Ali Road, Delhi
Key Dates	
Document Purchase Start Date and Time	**31.05.2022 11:00**
Document Purchase End Date and Time	**21.06.2022 15:00**
Last Date and Time for receipt of pre-bid queries	**07.06.2022** Before **15:00**
Pre Bid Meeting Date, Time and Location*	**09.06.2022 15:00** at Oriental House
Last Date and Time for submission of Bids	**21.06.2022 15:00**
Date and Time of Eligibility Bid Opening	**21.06.2022 15:30**
Opening of Technical bid	Will be communicated
Presentation by Qualified Bidders	Will be communicated

General Details	
Opening of Commercial bid	Will be communicated
Declaration of L1 Bidder	Will be communicated
Payment Details	
Tender Fees (INR)	INR 5,000 (Rupees Five Thousand only) by NEFT/ crossed Demand Draft/Banker's Pay Order in favour of "The Oriental Insurance Company Limited" payable at New Delhi. The RFP Document Price is non-refundable and inclusive of taxes *(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)*
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
Bid submission to Tender	**21.06.2022 15:00**
Contact details of e-Tender service provider	GeM Portal
Contact Information	Deputy General Manager, Information Technology Department, The Oriental Insurance Company Limited 2nd Floor, Head Office, Oriental House, A-25/27, Asaf Ali Road, New Delhi – 110 002 Tel: +91 11 43659201 E-mail: tender@orientalinsurance.co.in

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

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,
A - 25/27, 'Oriental House', 2nd Floor,
Asaf Ali Road, New Delhi – 110 002

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. 5,000/- (Rupees Five 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 in favor of "The Oriental Insurance Company Limited" payable at New Delhi. **Tender fee is inclusive of all taxes**.

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

1.6 Eligibility Criteria

S.No.	Bidder Eligibility Criteria	Supporting Documents
1	The Bidder should be a Registered Company in India under the 'Companies Act' and should be in existence in India for more than three (03) years as on bid submission date.	Copy of the Certificate of Incorporation issued by Registrar of Companies.
2	The Bidder should have had a minimum turnover of INR 200 crore in each of the last three financial years (2018-2019, 2019-2020 and 2020-2021).	Copy of Audited Financial statements for the financial years (2018-2019, 2019-2020 and 2020-2021) And CA Certificate
3	The Bidder should have a positive Net-Worth in each of the last three financial years (2018-2019, 2019-2020 and 2020-2021).	Copy of Audited Financial statements for the financial years (2018-2019, 2019-2020 and 2020-2021) And CA Certificate
4	The bidder should not be debarred / black-listed by any Government or PSU enterprise in India as on date of the submission of RFP.	Undertaking to this effect to be submitted on Company Letterhead as per Annexure 2.
5	The bidder should be an OEM or a certified or authorized agent/ reseller/ partner of the solution offered Product	Manufacturer's Authorization Form
6	The bidder should be a cloud service provider or a certified partner of cloud service provider. In case of a Bidder, who is not a Cloud service provider, bidder should have agreement with cloud service provider to host service on cloud and should have back-to-back support agreement with the cloud service provider.	Manufacturer's Authorization Form

S.No.	Bidder Eligibility Criteria	Supporting Documents
7	As per the Government guidelines on Procurement bidder needs to submit the Annexure 17 – Land Border with India	Bidder needs to Submit Annexure 17 - Land Border with India on letter head dully signed by Authorized signatory
8	Bidder should have its own Support center for Telephonic and Remote Assistance Services in Delhi, Mumbai / Navi Mumbai	Self-Declaration along with the details of the support centers in Delhi, Mumbai / Navi Mumbai.
9	The Bidder must have developed the Portal and Mobile app in any one BFSI/Government in India. The Portal and Mobile app must be live and running as on the date of submission of this RFP and must be catering of atleast 30 lakhs transactions per year.	PO / Contract copies with completion Certificate specifying the no of transactions in last financial year Or Credential Letter from client specifying the no of transactions in last financial year
10	The bidder must be CMMI level 5 Certified Company and the certificate should be valid as on date of bid submission	Copy of certification needs to be submitted

S.No.	OEM Eligibility Criteria	Supporting Documents
1	Proposed Cloud service provider should be MEITY (Govt. of India) empaneled	Copy of MEITY Empanelment
2	The Cloud Service Provider should have Public Cloud Service for a minimum period of three (3) years in India as on the date of the Tender.	Letter of confirmation from Cloud Service Provider
3	**Application Monitoring Solution:** The Proposed Application Monitoring solution on cloud should be implemented & Operational for atleast one BFSI in India	Relevant credential letter for the stipulated criteria Or Bidder should provide Purchase Order(s) together with the project completion / installation report duly signed & sealed by the respective Bidder's customer (The Purchase Orders & the installation /Project completion reports should have dates).
4	As per the Government guidelines on Procurement all OEM needs to submit the Annexure 17	OEM needs to Submit Annexure 17 on letter head dully signed by Authorized signatory

S.No.	OEM Eligibility Criteria	Supporting Documents
5	**Automated Disaster recovery Solution:** The Proposed Automated Disaster Recovery solution on cloud should be implemented & Operational for atleast one BFSI in India	Relevant credential letter for the stipulated criteria Or Bidder should provide Purchase Order(s) together with the project completion / installation report duly signed & sealed by the respective Bidder's customer (The Purchase Orders & the installation /Project completion reports should have dates).
6	**API Gateway:** The Proposed API Gateway solution on cloud should be implemented & Operational for atleast BFSI in India	Relevant credential letter for the stipulated criteria Or Bidder should provide Purchase Order(s) together with the project completion / installation report duly signed & sealed by the respective Bidder's customer (The Purchase Orders & the installation /Project completion reports should have dates).
7	**Password Less Authentication:** The Proposed password less Authentication solution should be implemented in at-least one BFSI in India	Relevant credential letter for the stipulated criteria Or Bidder should provide Purchase Order(s) together with the project completion / installation report duly signed & sealed by the respective Bidder's customer (The Purchase Orders & the installation /Project completion reports should have dates).
8	The cloud infrastructure provider should have presence in at least 2 cities in India and should have below certifications 1) ISO 27001 2) ISO 27002	Valid Document / Certificate needs to be submitted which are valid on bid submission

S.No.	OEM Eligibility Criteria	Supporting Documents
	3) ISO/IEC 27017:2015 4) ISO 27018 5) PCI- DSS 6) ISO 20000-1 7) STQC	
9	An **external testing agency** with experience of functional testing of Core application in BFSI India. Experience should cover areas of core application functionalities (either a direct hire or subcontractor)) is to be hired by the Bidder for conducting the functional / UAT testing of the developed Portal and Mobile app. Testing agency should have field level pre & post data migration testing experience on core application and this experience should be with use of tool.	Relevant credential letter for the stipulated criteria Or Bidder should provide Purchase Order(s) together with the project completion / installation report duly signed & sealed by the respective Bidder's customer (The Purchase Orders & the installation /Project completion reports should have dates).
10	**Load balancer: -** The proposed Load balancer should be implemented & Operational for atleast one BFSI in India	Relevant credential letter for the stipulated criteria Or Bidder should provide Purchase Order(s) together with the project completion / installation report duly signed & sealed by the respective Bidder's customer (The Purchase Orders & the installation /Project completion reports should have dates).
11	**HSM & KSM:** The Proposed HSM & KSM solution should be implemented & Operational in at-least one BFSI in India	Relevant credential letter for the stipulated criteria Or Bidder should provide Purchase Order(s) together with the project completion / installation report duly signed & sealed by the respective Bidder's customer (The Purchase

S.No.	OEM Eligibility Criteria	Supporting Documents
		Orders & the installation /Project completion reports should have dates).

Note:

i. Bidders need to ensure compliance to all the eligibility criteria points.

ii. In-case of corporate restructuring the earlier entity's incorporation certificate, financial statements, Credentials, etc. may be considered.

iii. 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.

iv. Purchase orders without relevant organization confirmation through a credential letter will not be considered as credentials.

v. If an agent submits a bid on behalf of the Principal/ OEM, the same agent shall not submit a bid on behalf of another Principal/ OEM for the same solution.

vi. Proposed solution need not be the proposed version of the solution

vii. If a bidder submits bid on behalf of the principal/OEM, the same bidder shall not submit on behalf of another principal/OEM in this tender.

viii. The branches being considered in the criteria should be per BFSI and not cumulative across BFSIs.

ix. BFSI - Banking, Financial Services and Insurance organizations, including regulatory authorities, in India.

x. 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 a RFP, either the Indian agent on behalf of the Principal/OEM or Principal/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 bid on behalf of the Principal/OEM, the same agent shall not submit a bid on behalf of another Principal/OEM in the same RFP for the same item/product.'*

1.7 Project Timelines

Project Timeline is as follows:

S.no	Activities	Timelines (T- Date of Purchase order)
	Phase 1	
Planning Phase		
1	• Detailed System Study, finalization of detailed list of activities, scope and duration of each of the activity and • submission of detailed project plan • Deployment Plan Document • Change Management Methodology Document	T+ 4 weeks
Requirement Gathering & Prototype		
	• The Vendor shall create 3 designs for the portal & each design shall have a home page and two inner pages. From the 3 • created designs, either one or a mix of designs will be selected which will then be used for the final development. • Detailed SRS Document • Detailed Use Cases and Activity diagrams • High Level Architecture Document • Techno – Functional Risks and Mitigation Document • Functionality Traceability matrix • High Level Design Document • Low Level Design Document • Test Plans	T + 10 weeks
Development		
3	• Development, Testing and Presentation of the Final version incorporating above feedback • Comprehensive Test Cases Document • Release Notes	T + 30 weeks
Testing		
4	• Training and UAT • UAT and Test Reports • Performance Test Report • Security Testing/Review Report • Safe to Host Certificate • Self-Audit report for Compliance with GIGW guidelines.	T + 35 weeks

	• STQC Certification	
Training and Knowledge Transfer		
5	Training as detailed in the RFP annexures	T + 39 weeks
Go-Live		
6	• Go-Live • Security Guide • User Management Guide • Content Management Guide	T + 40 weeks
Phase 2		
	Calculation of Premium and Quotation generation directly from Portal	T+45 weeks
	• Underwriting Logic from Portal only	T+52 weeks

The progress in the project implementation will be closely monitored and reviewed periodically by the ccommittees as decided by OICL.

Escalation Matrix

OICL as well as the Bidder will decide an escalation matrix to resolve any issues that may crop up during 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.

2 Scope of Work

The corporate web portal of OICL is currently managed by an outsourced agency and developed on liferay platform. OICL wants to develop the new website, the underlying Portals and the mobile app which also includes development of new functionalities, migration of existing portal features and contents and get all these hosted in the Private Virtual cloud with Disaster Recovery option in place. The bidder has to provide the technology solution which would also include implementation of the final Portal architecture. This would involve redesigning and developing the OICL web portal with corporate theme design its mobile app following the latest web trends including migration of information of existing pages, restructure overall content with proper tagging to make the screens reader friendly.

The new enterprise portal should have all those features/modules (with new features) present in the existing portal of the OICL. Key Areas for consideration and features to be implemented are as mentioned in this RFP (details of any other considerations and sub-features within these Core considerations and features to be discussed and finalized during implementation).

The Oriental Insurance Company Limited proposes to develop its corporate web portal and its mobile app to fulfil the following objectives.

1. To improve system scalability for more users, more traffic and transactions.
2. Easy integration with external services.
3. Improve the security.
4. To ensure compliance with various Guidelines.
5. To improve the electronic presence to public in an attractive & user-friendly manner.
6. To organize the contents in a logical and intuitive manner.
7. To integrate "easy to use" content management system for easily managing overall content of the website and mobile app. Adding new information or removing existing/old information should be simple.
8. To restructure content of the website and mobile app to make it more user friendly so that information is easily accessible.
9. Provide a personalized experience to web portal visitors based on user insights, category and interest.
10. To make site accessible on all platforms like desktops, laptops, tablets, I pads, mobile phones, other hand held devices etc. as well as to make mobile app accessible to all type of devices.
11. To improve the website in such a way that adoption of new technologies will be easier and reduce go-to market time. On the same hand all the existing functionalities needs to be cover in the new developed solution with captive premium calculation and policy issuance

The information shall be easily searchable on the site and the website should be optimized and scalable with capability to handle increased volume of data and visitors.

SI/MSP/CSP to provide IaaS model of hosting for the web application only through micro-service and containers-based architecture support that give the Department the flexibility and portability to move data and workloads in and out of different clouds, to deploy more quickly, and to manage applications

and data across environments. The solution to architected keeping in view that minimal vendor locking especially from cloud service provider point of view is achieved.

2.1 Existing Setup

OICL is ahead of its peers in the industry in adopting information technology. It has its own software development team that manages payroll, PF, website and other miscellaneous IT systems used in the company.

To bring uniformity, security and centralized access OICL has adopted integrated non-life insurance application software, named INLIAS, with the help of a technology partner, M/s Azentio. INLIAS is running successfully in more than 1000 operating offices.

The INLIAS application serves the entire business requirements of the OICL. Its scope covers from underwriting, accounting, claims processing, report generation and reinsurance requirements.

The company has set up Two-way Disaster Recovery Site in Active-Active Mode. The core-insurance application is served from primary Data Center and all non-transaction reports are served from secondary Data Center.

The Company has also launched state-of-the-art web portal in Sept 2009 through which customers can transact, make payments and track the status of various transactions. The portal has login facilities for retail customers, employees, corporate brokers and agents.

OICL has various other centralized applications like email, Desktop Management Suite, VC, SAP Investment management, Peoplesoft HRMS etc hosted at its Data Centers at Vashi and Bengaluru.

The Web Portal was launched in Sep 2009 and revamp in 2015. PwC has worked with OICL as a system integrator to implement its enterprise-wide service delivery web portal. The Portal solution is integrated with the core INLIAS insurance application for various business transactions and queries. The Portal solution also has provision for a secure, industry standard e-payment gateway. OICL"s technology architecture vision for this Portal solution is on a “Service Oriented Architecture Model”. PwC has implemented Sun Java System Portal Server and Sun Java Composite Application Suite ("JCAPS") as the SOA-based integration platform

The mobile app was launched in 2015. PwC has worked with OICL as a system integrator to implement OICL Mobile app which is running successfully on all type of devices.

2.1.1 Existing Stakeholders of Portal and Mobile app

2.1.1.1 Customers

Customers have a personalized dashboard for performing functions such as purchase of new policies, renewal of OICL policies as well as other company policies, Intimation of Claim, filing of Documents, registering and Search grievance, view transactions, view saved proposals, register policy, edit profile, view existing policies, online payment of premium by net banking, debit cards, credit cards etc.

2.1.1.2 Corporate Customer

Corporate Customers have a personalized dashboard for performing functions such as new purchase, renew, edit profile, search claims, provision for marine declaration, view CD Account details, Transactions etc.

2.1.1.3 Agents / POSP

Agents have a personalized dashboard for performing functions such as new purchase, Renewal of OICL as well as other company policies, edit profile, search claims and policies, Agent Documents, view communications and Discussions, view saved proposals etc.

2.1.1.4 Brokers

Brokers have a personalized dashboard for performing functions such as new purchase, Renewal of OICL as well as other company policies (Motor), edit profile, search claims and policies, view communications and Discussions, Check Renewals etc

2.1.1.5 Dealers

Dealers have a personalized dashboard for performing functions such as new purchase and renew only for Motor policies, edit profile, search claims and policies, view communications, CD Account Balance, Bulk Upload Facility, status of claims etc

2.1.1.6 TPA (Third Party Administrators)

TPA's have a personalized dashboard to perform jobs such as view premium, service charge details, policy details, view communications, edit profile etc.

2.1.1.7 Surveyor

Surveyors have a personalized dashboard to perform jobs such as edit profile, view pending tasks, check the status of fees paid, completed tasks, alerts etc.

2.1.1.8 Advocate

Advocates have a personalized dashboard to perform jobs such as edit profile, view pending tasks, check the status of fees paid, completed tasks, alerts etc.

2.1.1.9 Pensioner

Pensioners have a personalized dashboard to view the pensioner corner and latest updates.

2.1.1.10 Employee

Employees have a personalized dashboard to enable them to edit profile, view updates, employee search, perform and assign tasks, participate in Discussion Forum, search Proposals, intimate claims, register grievance, Guest house booking, online payment, view circulars etc.

2.2 Current Scope

The scope of work for the Development of Corporate portal and Mobile app and its maintenance would include but not limited to supply, install, development, implementation, and maintenance of Corporate Web portal and Mobile app at virtual Private cloud. The broad scope of work is as below

1) Bidder needs to develop the new Corporate Web Portal and Native mobile app covering all the existing functionality and the new functionalities as mentioned in the RFP and also finalized in the SRS stage.
2) Bidder needs to factor the application and database on the virtual private cloud at cloud space provider location
3) The bidder needs to factor the cloud (Infra as service) for DC and DR both location
4) Bidder needs to Design, supply, size, implement and maintain the API gateway for all third-party API consumed by the Portal.
5) Bidder needs to Design, supply, size, implement and maintain the Automated disaster recovery Tool and Application performance Management tool for Portal and Mobile app
6) Program Management of the entire implementation and facility management
7) Facilities Management (including AMC, ATS and other support services)
8) Conduct periodical DR Drills (a minimum of one in every Calendar quarter).
9) Solution should have a stable environment, clean and modern design that meets the latest UX and UI trends
10) The web-based solutions need to be built on a single code base that automatically adjusts to screen sizes, performs effectively on desktop (including wide screens), laptop, mobile, and tablet across all operating systems and multiple browsers.
11) The color palette used in the design phase should be based on the corporate colors of the OICL.
12) The solution should have multi-lingual interface
13) The solution should be intuitive, well-organized, aesthetically pleasing, visually compelling and representation of the excellence that our clients expect.
14) Simple user interface that is easy to navigate
15) All pages should have print version
16) The solution should follow the “3 clicks” rule, i.e., the user should be able to reach any specific piece in not more than 3 clicks

17) The solution must be viewable on multiple platforms, resolutions and browsers
18) The solution should deliver a consistent and delightful Customer Experience
19) Underwriting logic needs to be developed at Portal and Mobile app without having any dependency on Core application
20) Bidder needs to onboard a Third party agency for doing the UAT and Data migration testing
21) It is the responsibility of the Bidder to maintain all the logs i.e. Transaction log, application logs, DB logs etc. as per the guidelines issued by RBI. The Logs should be maintained 6 months online, post which, the logs should be archived on tape. Bidder is required to perform the configuration at application and hardware level in order to push the requisite logs to OICL SIEM and other security solutions for analysis.
22) The Bidder is required to conduct Benchmarking and stress testing of the new cloud infra.
23) Design, Size, supply, implement, commission and maintain the technical solutions and new initiatives like:
    a. Password less login
    b. Chatbot

The above is only an indicative list of tasks expected out of SI. The scope extends to all that is essential to discharge the role of a System Integrator, whether or not stated expressly except to the extent so explicitly excluded

2.3 Additional Items

All customizations and functionalities presently available shall be retrofitted and made available in the new customized portal and mobile app

Bidder needs to quote for additional 100 days of man efforts which will be utilized by the OICL during contract period for doing any additional integration of customization. OICL can opt for additional man efforts on the same price once the same are exhausted.

2.4 Project Phase

The complete project needs to be undertaken by the bidder in a phased manner as follows:

Phase 1 - Perform requirement gathering and develop the portal and mobile app with all other line items mentioned in current scope section **except underwriting engine through Portal and calculation of Premium/ schedule and quotation from portal**, along with setting up of different environment like Development/ UAT/ Production/ DR environment, deployment of new version for testing, UAT, training and Go-live.

Phase 2 - Bidder needs to develop and implement the logic of **underwriting through Portal and calculation of Premium and quotation & Policy Schedule generation from portal without taking the same from Core**

Phase 3 - Sustenance for the remaining contract period for all in scope items. The sustenance will start from the day Phase 1 will go live. There will be stabilization period of 3 months after Phase 1 go-live. The FM resource cost will start after stabilization period.

Bidder has the feasibility to run the Phase 1 and Phase 2 in parallel however OICL there should not be having dependency of Phase 2 on Phase 1 going Live.

2.5 Solution Design

The OICL requires the solution architecture to have the following minimum capabilities/ features:

2.5.1 END to END IT Architecture

The Solution should have a compatible end to end IT architecture covering

1. End to end solution architecture
2. End to end integration architecture
3. End to end implementation architecture

2.5.2 24X7 Availability

The Critical Business Solutions and other proposed solutions' design and deployment architecture should be such that the system is available to users 24 X 7 throughout the year without any down time even during OLTP, daily, monthly or annual closings, system maintenance, backups, report generation, MIS generation, and running of batch processes.

2.5.3 Liaison with existing OICL Vendor / OEM's

The bidder is required to liaise with the vendors of all existing applications, interfaces, delivery channel and network management of the OICL, and draw their support in integration, other applications/utilities, interfaces and hardware implementation. The bidder is expected to take the responsibility of managing all the applications, interfaces, infrastructure and coordinate with the OICL's vendors to meet required SLAs in addition to provide helpdesk support, facility management support, infrastructure support and system/database administrative services.

2.5.4 Bilingual

The new develop Portal and Mobile app should have bilingual capability minimum English and Hindi which can be extended to multiple languages as desire time to time by OICL and should be able to interact with other bilingual (English and Hindi) systems providing data in required format. The bilingual functionality should be provided as per regulatory guidelines and should be functional with go-live. The data storage need not be in Hindi or any other language. Only the presentation layer to the user has to be in in the language as desire by the customer.

Bidders are required to refer and comply to the Master Circular DBOD No. Rajbhasha BC. 25/ 06.11.04/ 2012-13 dated July 2, 2012 on the 'Use of Hindi'. The Master Circular has been suitably updated by incorporating instructions issued up to June 30, 2013 and has been placed on the RBI website (http://www.rbi.org.in).

2.5.5 Manuals / Documents

Bidder has to provide soft copies of Job Cards, User and Technical Manuals for all the functionalities/ modules/ hardware/ tools proposed for the solution separately. In addition, all the applications/utilities should have online contextual help with search option for all the users

Bidder has to follow worldwide practice and international standard for documentation for the entire system development life cycle. The documents and manuals should be kept up to date with proper version control during the entire contract period. OICL may require the bidder to deliver the following documents in hard and soft copy to OICL during development and implementation of the solution.

1. Detailed System Requirements Specification Document
2. High Level and Low-level architecture document
3. Customization retro fitment document
4. Techno-functional risks and mitigation document
5. Functionality traceability matrix which would provide details on the interdependence of technical components for the realization of a functionality
6. High Level Design document
7. Low Level Design document
8. Data migration strategy document
9. Interface strategy document
10. Test cases with results during UAT, SIT and any other test cases
11. Deployment plan document
12. Change management methodology document
13. Security guide
14. User management guide
15. Release notes
16. Impact matrix
17. All code develop for OICL needs to be documented and provided to OICL as well as any change in code during contract will be supplied to OICL

2.5.6 Integration with existing Applications

The bidder shall ensure seamless integration of the new portal and mobile app Solution with other existing/future Devices, applications/utilities, network, security, platform in the OICL's Data Center and Disaster Recovery Site etc. Bidder shall also be responsible for integration of newer peripheral applications that may be taken up during the project.

2.5.7 Projections

Below is the growth project which bidder need to consider during the design, size, implement, customize the solution

S.no	Particular	Window	Current	Year 1	Year 2	Year 3	Year 4	Year 5
1	Transactions Per day (Policy Sold)	00:00:00 - 23:59:59	5036	6044	7252	8340	9591	10550
2	Pek Transactions Per day (Policy Sold)	00:00:00 - 23:59:59	7884	11038	15453	20089	24107	26517
3	Total No. of registered Users	Till now	805632	966759	1160110	1334127	1534246	1687670
4	No. of policies sold through portal	F.Y 2021-22	1829366	Plan for atleast 20% increase	Plan for atleast 20% increase	Plan for atleast 15% increase	Plan for atleast 15% increase	Plan for atleast 10% increase
5	No. of Pageviews	F.Y 2021-22	66627020	Plan for atleast 20% increase	Plan for atleast 20% increase	Plan for atleast 15% increase	Plan for atleast 15% increase	Plan for atleast 10% increase
6	No. of users	F.Y 2021-22	2951091	Plan for atleast 20% increase	Plan for atleast 20% increase	Plan for atleast 15% increase	Plan for atleast 15% increase	Plan for atleast 10% increase

Particulars	Details
Total No. of New Customers per Year	47951 increase for last year, Growth of 7 % registered
Total No. of Affiliated Agents and YoY Growth	45965, growth of 18 % recorded
Total No. of Affiliated Surveyors and YoY Growth	3515, growth of 2% was recorded
Total No. of Affiliated Brokers and YoY Growth	317, growth of 9% was recorded
Total No. of Affiliated TPA (Third Party Administrator) and YoY Growth	19
Total No. of Associated Advocates	103

Total No. of Employees and YoY Growth	14996 (Actual employee figure is less)
Total No of Policies issued in a year in Core System	1996905, 1108212 (policies issued through portal FY 2020 and 2021 resp.)- downward trend due to low vehicle sales/GDP w.r.t corona/lockdown
Concurrent user	Current 1500 , YOY 20%
Pageviews in FY 2021-22	6,66,27,020

2.6 Detail Scope of Work

Detailed Description of the envisaged scope is enumerated below. However, the OICL at its discretion reserves the right to change the scope and phases of the RFP considering the size and variety of the requirements and changing business conditions and requirements

2.6.1 Phase I - Requirement gathering and develop the portal and mobile app with all other items

As part of this phase bidder needs to requirement gathering and develop the portal and Mobile app as per the requirement using all the latest technologies as mentioned in the RFP. The responsibility of the bidder shall include designing, sizing, procuring, development, customization retrofitting, configuring, parameterizing, implementing, training and maintenance of all the in-scope items that includes the Software Development Life Cycle (SDLC) activities covering at minimum the scope mentioned in this RFP

2.6.1.1 Requirement gathering

Bidder needs to coordinate will all the stake holders of the OICL and needs to develop a System requirement specifications document for portal and Native mobile app covering atleast below activities: -

1. Needs to finalize the parameters
2. Needs to finalize the UI/UX
3. Need to finalize the approval flow and all other flow of the module like Policy issuance, customer flow, claim flow, Underwriting flow, agents flow, brokers flow etc.
4. Bidder needs to take to take sign off of the OICL on the SRS
5. During SRS bidder needs to incorporate all the security related features
6. The Bidder is expected to study the existing portal and mobile app to assess the existing structure, content and user interface. The Portal and mobile app features, assistance and other items include, but not limited to, the functions and features defined in this RFP.

7. During requirement specification phase the bidder will have the responsibility of collecting requirements from OICL in the light of Business requirement. The selected bidder would study various department requirements and create a SRS document including migration strategy document. The SRS preparation should include rapid prototyping in the form of detailed screenshots of all interactions. OICL will sign off the on the screenshot and the SRS document. The Portal design will be carried out only after the SRS has been approved by OICL.
8. The Bidder shall device the system for data preparation/migration from existing portal and mobile app into the new Portal, wherever necessary.
9. Following are the broad level indicative minimum functionalities necessary for the Portal and mobile app. The bidder should ensure that all the current and future finalized functionalities should be customized in the new solution. These requirements are further detailed in RFP
10. Responsive User interface (Single Page Application architecture) that creates an interactive and engaging user experience
11. Build the UX for all mentioned functionalities of portal and mobile app
12. Review and finalize detailed functional, technical, integration and non -functional specifications
13. Architecture design for a scalable, highly available, reliable, secure performing solution
14. Workflow Design and Rule Design with user interfaces
15. Middleware architecture to support service enablement and integration
16. Data Model, data migration and synchronization mechanism design
17. Report Design as per requirements including the existing
18. Architecture of proposed web and mobile Portal should be both horizontally and vertically scalable for the 100% YOY business growth and 50% growth in number of users over 2 years
19. Providing User Logins based on mobile nos. or some other authentic criteria. These logins will show all policies pertaining to user at one place.
20. Use of Icons or graphics in selecting services will definitely add to UX.

2.6.1.2 Development of Portal and Mobile app

Bidder will be responsible for the development the portal and mobile app end to end from the scratch by adopting below mentioned technologies. However. **Bidder needs to note that OICL is not looking for any COTS / LOW Code/No Code platform on which bidder do customization.** OICL is looking for a full fledge development. Bidder also needs to note that bidder can use any or combination of below mentioned technologies for development

The Bidder needs to provide all statutory and regulatory reports as required by the regulatory institutions. OICL will not pay any additional customization costs either for gaps observed as given above and/or gaps observed for statutory or regulatory reports as required by the OICL.

The Bidder will have to provide the OICL weekly progress reports on the bugs/problems reported/points taken up with schedule of date of reporting, date of resolving, and status for all kind of bugs and problems whether reported by OICL or Bidder staff.

Customizations would be with respect to the proposed solution and interfaces that the OICL proposes to implement through the selected Bidder.

The OICL may require the Bidder to address additional requirements that are other than the following:

- Bug fixes
- Gaps found during base version testing

The Bidder will ensure that gaps pointed out by the audit and inspection teams, statutory and regulatory bodies, consultants or any other third-party agency engaged by the OICL will be immediately resolved.

The Bidder shall resolve gaps by proposing a suitable work around or customizing the proposed solution by way of modifications/enhancements, as necessary, to the proposed software solution.

The Bidder shall provide all statutory, regulatory and ad hoc MIS (Management Information System) reports as required by the OICL in the desired format during the initial phase of customization process.

The Bidder shall provide for all subsequent changes to reports as suggested by the statutory and regulatory bodies from time to time immediately to the OICL at no additional cost to the OICL during the contract period.

The Bidder will give adequate time to the OICL for reviewing the gap report

The Bidder will incorporate all the suggestions made by the OICL to the gap report.

The Bidder will ensure that they have the necessary infrastructure and people in place to resolve all the gaps within the timelines agreed, for the implementation and roll out.

The cost of all customizations as mentioned above is required to be included in the price bid and the OICL will not make any additional costs for such effort till project goes live. While costing the customization effort required, the Bidder should exclude the effort required from the OICL.

The Bidder is expected to document all gaps observed by the OICL at various stages of implementation including their solution and monitor and track the status of the same throughout the implementation

Bidder needs to note that all the technologies used by the bidder needs to license properly and in adequate number with proper road map and OEM support for the contract duration. All the cost of the license and support needs to be factor by the bidder in the commercial bill of material. OICL will not be responsible for providing any Licenses or any cost later on.

S.no	Description	Technologies can be used
1	Platform Installation & Configurations	1. Frontend to be in React / angular JS and latest Javascript Library like Tailwind CSS and Material U 2. Backend services to be in latest stable version of Spring Boot, express js, node js

		3. DB to be any open source or any RDBMS or combination of both however there has to be a proper OEM support and road map of the DB which needs to be submit with technical proposal 4. Provision to support No SQL and Big data requirements (support for MongoDB / Cassandra 5. Microservices orchestrated via Kubernetes 6. Access any data flexibly and easily: Access data in multiple formats (including CSV, Excel, and JSON), multiple sources (including object storage, Oracle Database, MongoDB, PostgreSQL, and Hadoop), and multiple locations (on premises, Cloud, and other clouds). 7. Design should support Auto scaling (Up & Down) of compute based on metrics (CPU & Memory) & time/schedule based to align with business demand like month end peak, quarterly & annual peak. 8. Support all current and future technology like Analytics, Blockchain or future technology On-Demand basis. 9. Integration platform should be implemented using SOA and must support ESB
2	Search Capabilities	Search capabilities on top of database Search capabilities using Elastic (ELK) Stack -Powerful search for documents and results living in websites, applications, and workplaces.
3	Devops	1. (CI/CD -Continuous Integration/Continuous Delivery) tools like Jenkins etc., 2. version control through Git / Github, 3. Log data analysis from any source and create helpful visualizations for data analysis through storage with Elastic search, processing and data collection with Logstash and visualization with Kibana (ELK Stack) , 4. Implementation of microservices deployment and orchestration tools like Kubernetes/Docker Swarm
4	Security	1. Compliance of ISNP/ISMS guidelines 2. Project to use approved technology and meets all information security policies 3. Threat prevention, detection, and response with SIEM and endpoint security 4. VAPT/WASA 5. Encryption of data on volumes, disk I/O, and snapshots using industry standard AES-256 cryptographic algorithm. 6. In-transit control plane data is encrypted by using Transport Layer Security (TLS) 1.2 or later. 7. Integration with SIEM for log collection. 8. Integration with key manager for storing the keys
5	Development	1. Full stack development is to be done using open source enterprise Java frameworks like Spring Boot, express jss , note jss for backend

		and Frontend to be in open source frameworks like React JS and latest Javascript Library like Tailwind etc. 2. Mobile App to be a Native app and not tied to web portal but to be an independent platform 3. Develop portal applications and interfaces Front end, Business Logic development for existing LOBs like Motor & Health product, Commercial products (other than Motor & Health) – API's would be provided by OICL Team. 4. Develop middle ware logic and rules 5. Develop the database logic 6. Integration with existing systems and 3rd Party (Vahaan, IIB, Aadhar, NSDL, Payment Gateways, Banks), Communication (SMS gateway, SMTP gateway, WhatsApp Business API), Google Analytics, etc. 7. Web portal also to be developed as a Headless PWA -allowing sending a push notification 8. Integration with OEM and Aggregator services 9. Quote Generation to Policy issuance 10. New business, endorsement, renewal, claim, servicing 11. Content management Solution 12. Workflow implementation 13. Rules Engine migration based on the existing rules provided from Core PAS (INLIAS)for U/W, Pricing, Quotation 14. API Gateway implementation as mentioned in the RFP 15. The website to be compatible with the upcoming potential user front end, by adapting to Headless Architecture (Decoupled architecture) by providing data to be rendered in json/XML format and delivers it in the raw form to the front-end wherever required 16. Cloud Native MicroServices Architecture Implementation 17. Integration with existing ECM that is enterprise content management which is documnetum 18. Distributed Cache implementation 19. ETL implementation for data synchronization (De-Dupe check using parameters like name, father's name, age, dob etc. on Client Master table , Automatic Contactibility Tracing where proper mobile nos are only accepted by system) 20. Master Data Repository (local data mart) to support Analytics for Portal business 21. Digital Marketing (SEO (Search Engine Optimisation etc.) and Social Media integration capabilities (WhatsApp Business API) 22. Application Performance Management tool implementation as mentioned in the RFP 23. DevOps & DevSecOps implementation 24. Online Claims registration

		25. For Grievance Redressal existing system integration to be done which is provided by IRDAI. 26. BILINGUAL version to be there 27. Chatbot to be implemented for automated user grievance handing as mentioned in the RFP 28. Role based logins and dashboards for all stakeholders including Agent/intermediary role and Hierarchy Management using front end form. 29. Base one time data to be migrated from Core PAS/existing portal DB 30. There has to be a provision to restful API for integration with external services 31. Manual/Auto mode payment reconciliation and refund setup
6	Database	1. Bidder needs to customize the database as per the requirement finalized during SRS phase 2. Portal and Mobile App database will also be hosted on the cloud 3. Database and transaction flow should be design in such a manner that even through the core application is not available then also there should not be any downtime of the portal 4. Rule engine and calculation logic and its parameters needs to be define in database as per the core and all the changes made in core application needs to be done in Portal and Mobile also so maintain the even products across environment
7	Monitoring Tools	1. Cloud based API tool 2. Cloud based APM tool
8	Disaster Recovery	1. Cloud based ADR tool / DRaaS 2. DNS FAIL OVER / GSLB
9	DevSecOps	DevSecOps through Code Analysis , Automated Testing , Change Management , Compliance Monitoring , Threat Investigation , Personnel Training for security integration across all stages of the software development process chain, addressing security concerns at the very start of every stage has to be ensure 1. Insecure code, such as code vulnerable to SQLi, XXS,XXE; OR weak encryption Malicious artifacts such as IPs, domains and files Sensitive data or Secrets 2. Through DevSecOps Detect over different secret or sensitive data, such as keys, passwords, usernames, URLs, domains in various artifacts, like: Uncompiled application code Software libraries, such as Node.js npm packages Software deliverables such as Android apps Production artifacts such as logs and storage Containers

		3. Through DevSecOps assist in CICD hardening, such as GIT repository Hardening 4. Through DevSecOps able to detect secrets or sensitive data in various developer collaboration tools, such as Jira, confluence and Slack 5. Through DevSecOps must integrate directly with SAAS app accounts, such as GitHub, to scan all repositories under that account 6. Solution should scan code repos github, bitbucket, npm and more without granting special permission and this solution must not be open source solution 7. The solution must be tightly integrated with application security solution and there should be a unified management console.
10	Analytics on Cloud	Vendor/SI/MSP/CSP to enable accessing data sources across on-premises and the cloud infrastructure, model that data and provide business users with a simplified view of their data to enable interactive self-service BI and data discovery using their preferred data visualization tool
11	App Security	The Application Security (WAAP) solution must be zero touch configuration based on Contextual AI and ML based to protect the web applications and API. it must meet the following characteristics or specifications. Incorporate the following protection technologies & integration : • Web Application Protection • API Security • Bot Prevention • Application Vulnerability Virtual Patching & IPS The IPS function shall provide traditional signature-based protections for web-based CVEs (Common Vulnerabilities and Exposures). For the container visibility & admission control solution, there should be a unified management console.
12	Container Security	Solutions need to continuously scan the K8s clusters checking for vulnerabilities & malwares The solution must be able to identify vulnerable dependencies during image scan The solution must detect when a container is performing abnormal actions & must show all the processes based on the behavioral profiling. The solution shall be able to provide admission control by only allowing images to be deployed with code from approved registries

		The solution includes static code analysis for container images capable of detecting vulnerable dependencies, embedded credentials, overtly permissive. The solution supports the integration of the static code analysis into a CICD pipeline (including AWS Code Pipeline, Azure DevOps, Jenkins, GitLab, CircleCI, etc.) The solution must allow users to create custom rules and rulesets for assessing admission control scenarios without writing code The solutions must be able to block privilege escalation within K8s pods The solution should monitor all 'exec' on K8s pods and create detection alerts even if it's approved

The proposed solution should have stable environment, clean and modern design that meets latest UX & UI trends. The proposal should include the complete designs solution for the Portal & Mobile app. The following is an inclusive but not necessarily exhaustive list of the requirements, desired features, and deliverables for the Design Phase:

1. Conduct necessary user research and usability testing throughout the life of the project to achieve objectives.
2. Create design according to the world-class standards.
3. Propose minimum of 3 (three) unique design options (card based single page application) for the home/login page and templates that correlate with OICL's style and will be used throughout the application
4. Use intuitive, well organized, aesthetically pleasing, visually compelling design that represents excellence that OICL's clients expect from OICL.
5. Successfully utilize the latest web/mobile trends and techniques to attract technologically proficient users without alienating users who feel more comfortable with traditional methods of browsing.
6. The design shall refine the information infrastructure, which will:

- Prioritize content.
- Simplify discoverability
- Provide the best UX to users.

2.6.1.3 Hosting

Bidder needs to note that the application needs to host on cloud and needs to be managed by bidder. All the cost of the hosting all the environment as mentioned in the RFP needs to factor by the bidder in the Annexure 16- Commercial bill of material with proper details and break up. During selecting of the Cloud bidder needs to ensure below

1. Bidder needs to provide RTO – 60 mins and RPO - 30 mins
2. Bidder needs to host all the environment (DC, DR & Non-Production) on cloud
3. Data Centre and Disaster Site (DR) shall be in India but in different seismic zone
4. No separate charges for inbound or outbound data transfer-charges only for port hours consumed and not data transfer
5. Bidder needs to ensure that if at all during the contract period OICL wants to move any or all environment from cloud to On prem/or any other public cloud then the selected cloud and bidder should have the provision of the same
6. Bidder and cloud provider will be responsible for all time of security management like VAPT, WASA for any security breach.
7. The infrastructure, Storage should be offered as virtual private cloud- as a service. DC & DR set up must comply with all Indian regulatory guidelines defined for providing cloud-based services in India.
8. Bidder needs to note that for database, bidder is free to choose either to host the same as service from the cloud provider or manage the same on the infra which is taken as service from the cloud.
9. Bidder also needs to note that there should be a direct connectivity between OICL DC and DR to the cloud provider with a dedicated link. Bidder needs to provide the sizing of the same as part of the RFP and also needs to factor the cost of the same in Annexure 16- Bill of Material.
10. The link provide by the bidder has to be in Active – Passive at DC and DR.
11. Bidder also need to note that the link should be monitored and maintain by the bidder only and the link which will be provision by the bidder at DC should from different service provider.
12. The bidder will be responsible for provisioning of requisite network infrastructure (including switches, router, firewalls, and load balancers) to ensure accessibility of the servers as per defined SLA's. All the equipment's/Devices in the path have to be in HA mode.
13. The Internet connectivity should be available to the applications as per the SLA requirements Additional charges for Data Ingress or Egress will not be paid by OICL.
14. Cloud must be hosted in India including DC and DR in India, no network, and data sharing/replication to any data centre outside the boundaries of the country is permitted. The bidder will be bound by Indian law and Indian IT Act (Cyber Law). No data in any circumstances should be shared / copied / transmitted without OICL's consent / written permission of OICL and it should be as per the Indian IT act (Cyber Law).
15. The Cloud service provider should be certified to be compliant to the following control standards and all these certificate needs to be submitted in technical proposal with a valid date:
    a. ISO 27001 – Data Centre and the cloud services should be certified for the latest version of the standards
    b. ISO/IEC 27017:2015 – Code of practice for information security controls based on ISO/IEC 27002 for cloud services and Information technology.

c. ISO 27018 – Code of practice for protection of personally identifiable information (PII) in public clouds.

d. ISO 20000-9-Guidance on the application of ISO/IEC 20000-1 to cloud services

16. Bidder should consider high-availability (active-active) for Portal and Mobile app at DC & DR
17. The bidder shall propose hardware such that at any point in time during the contract period, the peak CPU utilization of compute should not exceed 70% at the Primary Data Center and Disaster Recovery Center and 80% for storage.
18. The data files along with archives and individual file storage should be hosted in India for primary and secondary copies
19. The cloud infrastructure provider should have presence in at least 2 cities in India
20. The bidder must provide the Application Deployment Architecture with diagrams, identifying components and specifications for each component with description. Description must detail the number of servers, specifications for each resource (Web server, Application, DB, File server, Resource Monitoring servers etc.), Operating System and configuration as well as function of each server, Network Bandwidth Requirements and Storage Requirements.
21. The bidder is responsible for actual sizing of the infrastructure as per the scope of work, activities and Service Levels and projections as defined in this RFP
22. The proposed infra should be IPv4 & IPv6 compatible
23. All IRDAI and Govt. Mandated existing and future guidelines including ISNP/ISMS/Cybersecurity

2.6.1.4 Content & Data Migration

Bidder will be designing the new database as per the requirement finalized during SRS Phase. All the data and content required in new database and portal and mobile app for running of the portal and Mobile app needs to be migrated by the bidder in the new database by coordinating with OICL and as well as the existing system integrator of OICL

1. Bidder needs to ensure that during data migration there should not be a downtime of application more than 10 hours.
2. Bidder needs to Establish a both way data transfer mechanism between New data store for changed data with other database (related to partner portal-GC and Vice versa) synchronization
3. Bidder needs to develop a data migration audit check report which needs to be submitted after each migration to OICL Testing team. Bidder needs to finalize the format of the same with OICL.
4. Bidder needs to ensure that all the data is intact during migration in terms of P&L and other policies and customer data.
5. Bidder needs to work closely with OICL's identified Data Migration Audit team and close all the gaps identified by the team

6. Bidder needs to finalize a Database migration strategy document in conjunction with OICL and take sign off from OICL.
7. It is the responsibility of the bidder to study the data architecture and schemas
8. Development of control reports during data migration is the responsibility of the bidder
9. The Bidder shall ensure that sufficient technical training is imparted to the data migration team of OICL with regards to the new application data structure, field mapping requirements, field validations, default values and gaps in field mapping reports
10. Data Mapping between the existing and new application
11. Transform and load the data into the proposed solution
12. Perform data cleansing and removing data insufficiency while migrating
13. Provide consistency check on the data loaded into the proposed solution and confirm that there is no data loss or error of data values
14. Bidder needs to coordinate with existing vendor for getting the data in the required format for migration
15. Data Migration for Portal and app is an intensive operation including migration of transaction related data, user credential data including customer identifier, key user contact information, token mapping, user rights/ privileges and access control, channel limits, favorites etc.
16. Based on the design philosophy between the legacy and the proposed applications and the resultant complexities, OICL may opt not to migrate some of the above data (for security information like user rights/ privileges and access control) but create it afresh in the new application. Bidder to ensure that other data is migrated smoothly.
17. The most important area related to migration other than transaction data in digital self-service channels are User Credentials for authentication, as it has a direct impact on the customers of the OICL and require their participation to some level. This is also a key aspect of change management and communication that the bidder is required to look into.
18. For the purpose of this RFP, Bidders are required to submit a detailed Migration Approach document as part of the Technical Bid detailing out the following:

- Overall Migration Plan
- Migration Approach including but not limited to Transaction Data, Profile data comprising of User Credentials etc.
- In case of discrepancy in data, Bidder will provide a dashboard wherein the customer wise confirmation on the required data done by RO will be reflected.
- Fall back/ roll back plan in case of any Disaster. Fall back/ roll back plan in case of any Disaster. In case of fall Back/Roll Back required in the event of unsuccessful migration/issues in the migrated application(s), the bidder is required to roll back/fall back to the previously stable version/platform/framework (reverse migration) at no additional cost to the OICL post approval/confirmation from the OICL.
- Dependencies/ Preparation/ Readiness required from the OICL

- It is advisable to the Bidder to propose an approach which will minimize the change.

19. Additionally, a list of contents provided by the OICL shall also be added to the web portal by the selected Bidder time to time during contract period.

2.6.1.5 System Integration testing

The OICL will require the successful Bidder to prepare a plan that details the methods and procedures that will be used to execute the test cases. On completion of unit testing of all modules by the portal and mobile app developer, the testing team will carry out a complete integration testing. During the SIT run, all the transactions and features will be verified along with interaction with all other external applications. The test run methodology will be developed and adopted after consultation between the Bidder and the OICL representatives. The Bidder will also conduct a Stress & Performance Testing of the Portal and mobile app as per the load mentioned in the RFP before deployment of the solution for production. The benchmarking and stress testing is detail in the RFP.

Bidder needs to submit the result and test cases used to do the Unit testing and SIT before starting the testing by the External agency. During SIT and Unit testing bidder needs to execute positive and negative both type of test cases

The bidder is expected to carry out periodic Security and Penetration testing on the portal and mobile solution and submit its report to OICL to ensure that the solution cater to the expected load specified in the requirement. Tool for doing the Security and Penetration testing should be provided by the Bidder.

As part of testing user needs to perform below:-

1. System integration testing
2. Performance Testing
3. User acceptance test support
4. Application Security Testing
5. Regression Testing
6. Defect fixes
7. VAPT/WASA
8. DC-DR Testing

2.6.1.6 Security

The Bidder shall devise the system for handling all security issues like handling authentication, role-based access control, portlet security, and web services security. The Bidder needs to secure connections between clients and the Portal and Mobile app, connections between the portal, mobile app and other applications as well as connections between the Portal and Payment Gateways. The security document requires to be approved before implementation. The Bidder needs to describe in a separate paper how the security can be implemented for the Portal. Bidder needs to fulfill all the compliance mentioned in Annexure 15 - Functional & Technical Specifications.

1. The website and mobile app should incorporate necessary security features against hacking and defacement.
2. The security design for the Portal and mobile app should follow the best practices for the websites, secured website, and enterprise portal/web servers as per the security policy of OICL, CERT-In/IRDAI Guidelines/Government guidelines.
3. All logins and payments transaction must operate on secure protocols. It should provide support for website security audit.
4. The portal should comply fully with the guidelines issued from time to time by Govt. of India.
5. The Bidder will arrange security audit of web portal from one of the empaneled agencies (by CERTIn) and clear the same, prior to “Go-Live".
6. The Bidder should assist OICL to formulate a security policy to address various security issues related to web portal and mobile app.
7. All development and solution proposed should be Compliance of ISNP/ISMS guidelines
8. Solution to use approved technology and meets all information security policies
9. Threat prevention, detection, and response with SIEM and endpoint security
10. VAPT/WASA
11. Encryption of data on volumes, disk I/O, and snapshots using industry standard AES-256 cryptographic algorithm.
12. In-transit control plane data is encrypted by using Transport Layer Security (TLS) 1.2 or later.

2.6.1.7 Data Encryption & Object Signing

a) All the interfaces between various applications and user are encrypted using appropriate protocols (such as HTTPS, IPSec, SSL etc.), algorithm and key pairs.

b) System should support 128/256/512 bit encryption for transmission of the data over the Internet.

c) Object signing and encryption of attachments (documents) should be compliant to published DeitY standards.

d) Proposed solution must be secured to both internal and external parties (such as through encryption)

e) The Network / Transport level should include Network Link Encryption (IPSEC) and encrypted HTTP session using TLS/SSL (HTTPS)

f) Business data should be encrypted in the database and DBA should not be able to read or modify it.

g) Audit controls, electronic signatures, data encryption and other methods should be used to assure the authenticity of transaction and other relevant data

h) Following events should be considered as security incidents: unsuccessful log-on, intrusion detection, malfunctioning of encryption facility, etc.

i) Should develop a procedure for archiving the log files and ensure security of the log files

j) Separate environment should be maintained for production, test and development to reduce the risks of unauthorized access or changes

   a. System should have the functionality to record all the administrator, user level activities including the failed attempts

   b. Should protect logging facilities and log information against tampering and unauthorized access

   c. Information security baseline document should be developed for all the infrastructure components such as database, operating system, router, switch etc. based on CERT-In technical guidelines and best practices.

   d. Provisions should be made for secure content management.

   e. Solution should ensure logs including at least the following:

      i. Authentication and Authorization events – logging in, logging out, failed logins. These should include date/time, success/failure, and resources being authorized, the user requesting the authorization and IP address or location of the authentication attempt

      ii. Logs for deletion of any data

      iii. Logs of all administrator activity

      iv. Logs of modification to data characteristics: permissions, location, field type

2.6.1.8 Securing Data at Rest

Data at rest in various Data stores would be protected by hashing (salt) confidential data in both transactional and warehouse data stores. The security for the transactional data stores to be ensured by vertical partitioning of the data.

2.6.1.9 Data Integrity

Data in transit (from external systems or between internal systems) or data at rest must be protected from tampering. The risk is from both external users and internal users (such as Database Administrators) who are close to the data at all times.

To handle the risks of data being tampered by the external users and during transit, API design must ensure checksum features and digital signatures to validate the data is secured. System shall ensure to validate integrity using the checksum and digital signature validations before processing the data.

To handle the risks of data being tampered by the internal users such as Database Administrators who have access to data, application shall be designed with the below principles:

a) All the data access must be enabled only through internal API / modules.

b) Each subject area can be packages into a persistence module that exposes domain specific methods to read, insert, update or delete the records

c) Persistence module shall abstract the underlying data base technologies, physical data models

d) Based on the current proposals, underlying technology used to store data could be in one of the possible ways:

   a. RDBMS store

   b. HBase column based store

   c. File store (e.g HDFS, XFS)

2.6.1.10 Load balancer

Bidder needs to design, size and implement Web Portal in such a manner that it will run from two or more servers using a load balancer to route traffic between separate instances on different servers. In the event of a problem with a server, the load needs to be transferred to the remaining servers, with no disruption to service or loss of data. Bidder needs to fulfill all the compliance mentioned in Annexure 15 - Functional & Technical Specifications.

Bidder needs to factor a load balancer as per the specifications provided in the RFP however the same will be on prem or dedicated on cloud that bidder can decided as per the solutioning. All the cost of the same with the ATS and AMC needs to be factor by the bidder.

Load balancer has to be factor in HA mode (Active – Active) in at both i.e DC & DR

2.6.1.11 Document Management

The portal will be equipped to provide document management capabilities like:

1. Uploading of documents (even bulk document upload)

2. No restriction imposed on the document type and volumes of documents being uploaded, provided underlying storage capacity available. The allowable size and formats for document uploads must be configurable.

3. Serve as a central document repository

4. Maintain document hierarchy and support document versioning.

5. The portal should have option and ability to allow authorized portal users to upload various documents, media to the web site:

   a. Photos (multiple images at a time)

   b. Videos (limited size)

   c. Files (all format files except executables)

   d. Facility of Geo tagging to be provided

OICL Is already having a document management system which is on prem from Documentum. Bidder needs to integrate the solution with the same software

2.6.1.12 Content management

The portal and mobile app should have a comprehensive content management system to support a variety of users. It should allow the administrator to create user roles and allow the setting up of access rights ranging from entire site to a specific page. The Content Management should be able to create and upload the pages daily/weekly/ or on frequent basis with appropriate Business flow required for authenticate Publications of content on site.

1. The content management system must be able to allow users with no knowledge of HTML to publish material to portal.
2. It must allow for workflow for the approval for that content.
3. The solution must manage multiple versions of files and documents.
4. The solution should allow any version of the file to be viewed.
5. The solution should provide facilities for archiving content and for managing old content.
6. The solution must provide browser-based facility for managing content.
7. The OICL should be able to create, read, update and delete content in any of the repositories. These content repository capabilities should support Industry standard.
8. The solution should support check-in, check out, revert functionality and version control.
9. The Solution should have an easy to use web interface to upload contents to the Internet Web Site, Secured Website and Enterprise Portal. Content developers with varying skill levels must be able to publish content quickly and easily for variety of purpose and audience.
10. Publishing must be quick and must result in immediate publishing of new content.
11. The solution should support various types of file formats like .doc, .ppt, pdf, picture files, webcasts, multimedia files, audio, video files, etc.
12. The solution must provide a tool for uploading variant file types-word, pdf, etc. For the same document which would then appear as one entity followed by choice of file types.
13. The solution should provide common document management features like check in/checkout, versioning and document reviewing.

14. The solution must provide automated workflows that route content through an approval process and also allow editing at each level. Approvers should be notified of content awaiting approval via email and pending action.

15. Every Department of OICL will designate a user as content publisher who will have rights to publish the content on the Portal Solution. Designated Officer of the respective department will approve the contents before publishing it on to the Portal.

2.6.1.13 Integration with Social Media

It will also provide features to integrate with social media so that the content can be shared on social channels by the visitors.

1. Enable the customers and agents to share their experience through blogs and allow others to read these experiences

2. Will enable collaboration amongst employees through discussion forums, blogs.

3. Will be equipped with ability to enable login to the portal with the help of the Visitors Social Site ID.

4. Creation and /using the existing business Account for/and Integration of Social media platforms like Whatsapp/facebook/twitter through implementation of voice or chat based app

2.6.1.14 Search capabilities and Optimization

The system shall provide a full text search for all the content. This shall be able to search in all the links, sub-links, sub sub-links and shall provide links where the searched word or phrase is present. On clicking the link, the content shall be displayed

The portal will facilitate the Search Engine Optimization by providing an easy way to assign short and easy to understand URL"s. The system shall re-write the URL"s that are search engine friendly. The re-written URL"s shall be shorter and more relevant looking links to web pages.

Bidder also needs to ensure to include those key words which will be provided by the OICL so that the ranking and rating of the OICL in search engine will be among top searches

2.6.1.15 Web Analytics

The portal solution will provide analytics to understand the website traffic and the content /promotion performances, and should be able to integrate with tools such as google analytics

The portal will enable segmentation and targeting by the study of site usage basis the visitor"s pattern of accessing content on the portal, geo-location of the visitor etc.

2.6.1.16 Workflow Capability & Profile based functionalities on the fly

The Portal application shall provide reusable process workflows to help in the backend processing of policies. It must have the capability to configure rules with respect to any workflow process

It must enable easy to use administration facility with well-defined workflows for creating, approving and publishing the web contents. The finally published contents must then be syndicated to delivery system on-demand basis. The system shall allow different departments to have their own content libraries, workflow, templates and taxonomies.

The workflow must support the processes with

1. Publishing stages
2. Complex business rule support
3. Balancing of tasks across a group of users

The workflow capabilities must be configurable using Role based access to data and features/functionalities.

2.6.1.17 Redesign, Content Presentation

The graphic design of new web portal and mobile app should have a corporate look and feel commensurate with International standards.

The Bidder is expected to create a common style throughout our web portal through a new template to give the user a consistent look and feel while interacting with different web pages/applications. The Bidder is expected to create a user guide for our content authors to use as a reference when creating content so that it retains the look and feel of our template. The template needs to be responsive and mobile friendly.

Design and Content Management should support Extensive Web Site Analytics and Statistics. Traffic reports, visitor analysis, duration analysis, content wise analysis, top landing pages and top exit pages, other statistical reports should be available.

2.6.1.18 Mobile Application

Apart for web portal the OICL application should also be available in the mobile version. Some of the key requirements related to Mobile application, but not limited to, are mentioned below:

a) The Mobile Application should provide an intuitive and user friendly GUI that enables users to navigate and apply actions with ease. The GUI should be responsive with very little or no delays or time lag at launch or whilst navigating through screens.

b) It should enable ease of configuration and changes to existing GUIs, and support the introduction of new screens.

c) It should provide on screen tips and online help to aid users while interacting with it.

d) Should make use of data available in the existing database and reduce duplicate data entry

e) Incorporate analytics into mobile app, to track and identify users experience and actions.

f) Apps should be easily customizable and easy to Administer data in the database

g) Network level security, traffic should be encrypted using secured connectivity

h) Should support real time information via GPS availability

i) Should structure overall content with proper tagging to make them screen reader friendly.

j) Application should ensure Compatibility with all platforms such as windows, Android, Blackberry & Mac iOS etc.

k) Solution should develop resolution independent design structure i.e. Mobile Application should adjust itself automatically as per the screen resolution of the Mobile

l) Mobile Apps should work flawlessly across different platforms

m) There should be minimum use flash contents so that home page should be loaded quickly

n) It should not occupy excess client's Mobile RAM.

o) Should provide Role Based Access control

p) Should be able to capture and track all events at device and console.

q) Should come with mobile threat prevention and recovery system

r) Should support authentication using digital signatures

s) Should have facility to download and upload files.

2.6.1.19 Integration with Payment Gateways

The system is envisaged to have integration with payment gateways of the bank, to enable authorized Users make financial transactions, as per rights and privileges provided to him / her. The bidder is required to make the provisions for integration with such third party gateways and provide payment services, as per requirement of the system. Some of the key features of payment gateway are mentioned below:

a) Should support secure integration with Payment Service Providers

b) Should support a unified interface to integrate with all Payment Service Providers

c) Should support integration with Payment Service Providers using web services over secured protocols such as HTTP/S

d) Should manage messages exchange between UI and payment service providers

e) Should support beneficiary's payment transactions tracking against various services

f) Should support bank accounts reconciliation

g) Should provide and preserve all logs for all transactions performed through the Payment Gateway for future financial dispute resolution that might arise between entities and either beneficiaries or Payment Service Providers

h) Should maintain and keep transactions logs for time period required and specified by the financial regulations followed in country

i) Should support redundant Payment Discovery

j) Should submit Periodic Reconciliation Report to government entities

k) Should support transaction reports to monitor and track payments

l) Should support real-time online credit card authorization for merchants

m) Should support compliance with emerging trends and multiple payment options such as debit card, credit card, cash cards and other payment mechanisms

n) Should provide fraud screening features, alert mechanism

o) Should support browser based remote administration

p) Should support multicurrency processing and settlement directly to merchant account

q) Should support processing of one-time or recurring transactions using tokenization

r) Should support real time integration with SMS and emails

s) Should be compliant to standards like PCI DSS

2.6.1.20 Openness

Adoption of open API, open standards and wherever prudent open source products are of paramount importance for the system. This will ensure the system to be lightweight, scalable and secure. Openness comes from use of open standards and creating vendor neutral APIs and interfaces for all components. All the APIs will be stateless. Data access must be always through APIs, no application will access data directly from the storage layer or data access layer. For every internal data access also (access between various modules) there will be APIs and no direct access will be there.

Whenever options are available, open source frameworks/components shall be used instead of proprietary frameworks/components. Use of proprietary products/components/frameworks must be via open APIs (if publicly available APIs do not exist, the MSP shall be responsible for creating vendor neutral APIs before any proprietary system can be used). Use of open source is critical to ensure OICL becomes secure and independent from the impact of changes in political relations with other countries.

Use of open APIs addresses two primary goals – loose coupling of components allowing independent evolution of each component without affecting the other and having a vendor/provider neutral layer allowing use of one or more providers and replacement of a system component with another without affecting other parts of the system. In addition to the above goals, having API driven approach allows test automation for automated regression testing, continuous re-factoring and tuning within an implementation, and better component level versioning and lifecycle management.

2.6.1.21 Software vendor neutrality

As per GOI policy on adoption of open source software, OICL shall prefer open source system (OSS) in comparison to closed source software (CSS). Specific OEM products may only be used when necessary to achieve scale, performance and reliability. Every such OEM component/service/product/framework/MSP pre-existing product or work must be wrapped in a vendor neutral API so that at any time the OEM product can be replaced without affecting rest of the system. In addition, there must be at least 2 independent OEM products available using same standard/API before it can be used to ensure system is not locked in to single vendor implementation

2.6.1.22 Architecture, Auto Scaling & Performance

a) The proposed architecture for the cloud service should be capable of auto scaling without any manual intervention for all the resources including but not limited to vCPU, vRAM, Bandwidth, storage etc.

b) The proposed architecture should Auto scale the cloud workload to meet high / unpredictable demands. In this context, provisioning of Load Balancing, amongst others must be an integral part of the proposed architecture / solution

c) Auto-scaling to be done based on defined rules and parameters e.g., CPU utilization and memory usage

d) Scaling should be done both vertically – by increasing the amount of memory available to each instance – or horizontally – by creating additional instances.

e) The Cloud platform should provide a way to track the billing based on utilization and service levels in a Dashboard

f) The architecture should have the inherent feature capability to auto scale the deployed application in the scaled up resources.

2.6.1.23 Scalability

For achieving massive scale it is critical that technology choices are kept simple, open, multi-vendor, and standards based. Following are key considerations that need to be followed at architecture level from the beginning to ensure technology scale:

a) Loose coupling through open stateless API and messaging

b) The system design shall be modular with clear separation of concerns at data storage, service and API layer. Adoption of open standards shall work towards the singular goal of interoperability.

c) Because OICL system is conceived as a ‘common platform’ on which many applications will be built/ interfaced, it is critical that all 3rd party interfaces be fully interoperable without any affinity to platforms, programming languages, network technologies. Such open interoperability is an absolute requirement for OICL system.

d) In addition, even within the OICL solution, all components must be loosely coupled using open interfaces (APIs) ensuring interoperability across components and subsystems.

2.6.1.24 Design and development of Intelligent Data Analytics dashboards

Dashboard for Data Analytics: An Analytical suite is needed to manage and monitors the new digitalized platform. This will help in knowing the activity on digitalized portal and for research studies

Management facility inbuilt with the site Design and Content Management should support Extensive Web Site Analytics and Statistics to be provided. Traffic reports, visitor analysis, duration analysis, content wise analysis, top landing pages and top exit pages, other statistical reports should be provided as per company's requirements

The Solution shall have comprehensive settlement / reconciliation and complaint redressal mechanism.

The vendor shall provide complete technical details and specimen of the following MIS reports.

1. User wise Reports
2. Transaction-wise Reports
3. No of Registered/Downloaded Users
4. Reports based on filters such as user activity, customer status, range of date/time, status
5. Audit Trail Report
6. Provision to search for customers based on different search filters like name, mobile no, address, age, status and Account No

2.6.1.25 SSL Certificate or any Certificate or security component

Bidder needs to note that any SSL Certificate or any other certificate, software, security component which is required for Portal, mobile app or any other component of the RFP needs to be procured, deploy and maintain by the bidder. All these certificate and component has to be in the name of the OICL and must be handover to OICL

2.6.1.26 Ticketing Tool

As part of the development of portal and mobile app bidder needs to develop a ticketing tool also which will be used by the customer to log complain. This ticketing tool will be integrated with Portal, Mobile app, Chabot, Email and SMS gateway.

Bidder can either develop the tool or propose a readily available tool in the market but the tool will be hosted on the cloud and maintained by the bidder. The tool must cater below functionalities

1. Ticket Flow as finalized during SRS
2. Dashboard as finalized with SRS
3. Role based access
4. Escalation logic
5. Centralized reporting / MIS for all the modules suggested
6. Support to manage all types of operating system through one software
7. The proposed solution should provide flexibility of logging, viewing, updating and closing incidents manually via web interface.
8. The proposed solution should be able to provide flexibility of incident assignment based on the workload, category, or location.
9. The proposed solution must provide web-based knowledge database to store useful history incident resolution.

10. The proposed solution should provide built-in reporting functionality
11. The proposed solution should allow creation of surveys that allows systematic collection and analysis of customer feedback about service desk performance
12. The proposed solution should be able to log and escalate user interactions and requests
13. The proposed solution should provide status of registered calls to end-users over email and through web.
14. The proposed solution should have an updateable knowledge base for technical analysis and further help end-users to search solutions for previously solved issues.
15. The proposed solution should have the ability to track work history of calls to facilitate troubleshooting.
16. The proposed solution should support tracking of SLA (service level agreements) for call requests within the help desk through service types.
17. It should also have a graphical workflow designer with drag & drop feature for workflow creation and updation
18. In the proposed solution reports should be scheduled to be run and sent to administrators at specified times and intervals
19. In the proposed solution, reports should be viewed online
20. In the proposed solution, reports should be downloaded in CSV, PDF, TXT and XML formats
21. In the proposed solution, reports should be sent through emails
22. In Proposed solution ticket can be logged in the ticket tool based on the email send by the customer.

2.6.1.27 Phase 2- Underwriting Logic

As of now the underwriting logic is embedded in the OICL Core application which is provided by Azentio. OICL wants to reduce the dependency of the Portal & mobile app on Core application and also to reduce the to and fro of the data. All the underwriting logic needs to write in the new portal application. This logic needs to modify as and when there is some modification done in the logic at core application side. Also, this logic needs to update/ Modify whenever new products are launched. Bidder needs to note that OICL wants the underwriting logic to be written in such a manner that it can work as an standalone module if any / all the integrated application / modules are down or not available due to any unavoidable reasons. Premium calculation engine has to be built in the portal and the portal to be able to generate quotes and policy issuance independent of OICL core system availability. However, The transactions in portal has to be synched with OICL core /data warehouse on a real time / batch mode depending on availability of OICL core system based on common data standard and format

2.6.1.28 Application integration

The proposed architecture for Web Portal shall be Service Oriented Architecture (SOA) that best supports integration with other applications. The Bidder shall migrate or redevelop web services and methodology to integrate Portal and mobile app to other internal and external applications. This application Integration exercise may involve interaction of the Bidder with other application service providers. The Bidder will study, analyze the existing integration methods and finalize the integration technology after considering the system technology of other applications. The Bidder will be responsible for providing secure and efficient Integration of Portal to the following applications as well all other application which are in scope of the RFP, however this is only an indicative list and OICL will ask bidder to integration will other application which will be finalized in SRS or Implementation Phase:

S.no	Application
1	INLIAS (Core Insurance Business application of OICL)
2	Payment Gateway
3	Email
4	SMS Service Provider
5	IRDAI – IGMS
6	Web Aggregator
7	Broker Portal
8	Common Service Center Portal
9	Separate login for Bank insurance partner for Online issuance of our Policies
10	Separate login for Motor dealers for online issuance of our policies at dealer end
11	IVR
12	Whats app
13	HRMS
14	CRM

There will be some future application which bidder needs to integrator during contract period. It is the responsibility of the Bidder to provide these integrations by providing new source code in latest version and technology. It is the responsibility of the Bidder to provide any third-party utilities, connectors, or scripts for such integration without any additional cost to OICL.

2.6.1.29 Benchmarking

The Bidder will have to perform the benchmark for the purpose of this project, incorporating the proposed technology architecture for the applications within the scope of this RFP. The Bidder will have to do a benchmark on the hardware, sizing and architecture proposed for the applications specific to the application designed by the Bidder with due concurrence of OICL. **Benchmark needs to be validated & reported by reputed independent 3rd party who has the experience of reporting performance benchmark.**

The Bidder will have to perform a product benchmark at the benchmarking center as identified by the Bidder in the presence of OICL employees or its appointed officials or PMO resources. The objective of this exercise is to demonstrate that the proposed sizing, hardware and architecture meets the requirements and provides the required service levels in terms of number of the necessary transactions per second (TPS), user concurrency, Business Volumes and Growth Projections, along with the necessary number of concurrent transactions, total number of transactions in a 4 hour window, time taken for End of Day, batch processing and meet the required response time as expected by OICL. This benchmark should be carried out on the proposed hardware, sizing and architecture with the proposed version of the operating system, proposed version of the database system and the proposed version of the application system. The benchmarking exercise should be successfully completed within 2 months from the date of Go-live.

The Bidder should factor all the necessary costs for the benchmark, including the travel, lodging, meals for OICL personnel.

Any expenses incurred for the same would be borne by Bidder and under no circumstances the same would be reimbursed to the Bidder by OICL. The Bidder is expected to factor the all expenses linked to the benchmarking in the Bill of Materials.

The Bidder shall ensure that the solution provided and sized by the Bidder is capable of meeting OICL"s current and terminal year transaction and business volumes.

Bidder has to be study the load compute wise and during performance load testing bidders needs to generate same load according to the projection provided by OICL to certify the sizing, hardware and architecture.

All the benchmarking activities has to be done keeping in consideration of all type of customization of the OICL which are finalized during DRG phase.

During Benchmarking, the load generated by the bidder has to be in accordance with the transaction mix and the current setup of the OICL. The sign off should be taken from the OICL

All the benchmarking activities has to be done keeping in consideration of all type of customization & integrations of the OICL.

During Benchmarking, if it is observed that the required parameters are not achieved, then, bidder is required to augment the hardware within 2 months from the date of submission of Benchmarking report at no additional cost to OICL. Also, all terms and conditions mentioned in **Annexure 18 – Sizing Adequacy letter will be applicable.**

For generating the load, bidder needs to factor an appropriate load simulation tool for the duration of benchmarking only at no additional cost to OICL. Bidder needs to do the installation, configuration, maintenance of the same.

Stress Testing: - Bidder needs to do stress testing during implementation using the stress testing tool. Bidder needs to provide a report and take sign off from the OICL before going live. Stress Testing needs to be done on all layers of the solutions setup and if any deviations pointed out by the OICL, bidder needs to resolve the same before

2.6.1.30 Encryption, HSM, KSM & Digital Signature

The Bidder is required to design, supply, install, train, customize, test, implement, rollout and maintain the Security Module (HSM) as well as Key management solution and hardware at cloud as per the requirements of this RFP. Bidder needs to fulfill all the compliance mentioned in Annexure 15 - Functional & Technical Specifications. The bidder is also required to supply, size, implement and maintain the server hardware, Storage, OS, Databases and required to install the Security Module (HSM) as well as Key management solution. Bidder needs to provide Security Module (HSM) as well as Key management solution as a service in the cloud

Hardware Security Module

It is imperative to secure sensitive data and critical applications by storing, protecting, and managing cryptographic keys in a Hardware Security Module (HSM). The device should be high-assurance, tamper-resistant, network-attached appliance.

1) Store the private keys used for digital signing
2) Store document signer certificates for digital Invoice signing
3) Should maintain high availability within data center
4) Supply updates and upgrades including new versions of all the software licenses supplied as part of this tender during the entire contract period
5) Store critical crypto keys at the highest level of security. It will provide secure storage as well as secure digital signing operations such that Keys always remains in HSM hardware and never travels outside or stored in software in any form.
6) Accelerate Crypto operations to eliminate bottlenecks.
7) Guard against evolving threats and capitalize on emerging technologies including the Internet of Things (IoT), Blockchain and more.
8) Provide audit trails for all key material and crypto operation which can be used for auditing purpose.
9) Eliminate bottleneck of providing digital certificate on crypto tokens.

10) Act as Root of Trust for the Key Management Server

Key Management Solution (KMS)

KMS will be a hardened virtual appliance offering the industry leading enterprise key management solution enabling to centrally manage encryption keys, provide granular access control and configure security policies. It will manage key lifecycle tasks including generation, rotation, destruction, import and export, provide role-based access control to keys and policies, support robust auditing and reporting.

1) Every application that will be on-boarded to the service must have a unique cryptographic key associated with it for encryption/decryption which is to be stored in a Key Management Appliance Software secured with a FIPS 140-2 level-3 compliant Hardware Security Module at all times. Unauthorized access to the keys should be restricted. Considering interdependency and interoperability requirements on the solution the KMS and HSM should be from same OEM.

2) Proposed solution should allow encryption/decryption only after successful verification of credentials which should be certificate based or any other such secure robust mechanism not prone to tampering or eavesdropping

3) Detailed logging and audit tracking of all key state changes administrator access and policy changes. Support for multiple log formats (RFC-5424, CEF, LEEF) for easy integration that can be consumed by SIEM tools of OICL. Option to extract raw logs must be available.

4) Applications should be restricted by roles (user and application) to control who can encrypt decrypt or perform search operations.

5) Granular authorization capabilities that enable constraints to be placed on user operations based on specific key permissions.

6) Solution must be able to implement a Centralized Key Management Platform that would not only securely store the keys separately from the encrypted data but also manage the keys efficiently throughout their entire lifecycle separately on an external key manager which is owned and managed by the customer.

7) Solution must be capable to provide data-at-rest encryption for file/folder level encryption of on-premises data storage.

Bidder needs to note the all the keys for all the applications / hardware, OS, DB etc should be integrated with KSM and HSM.

Also, OICL is looking for the policy document generation from the Portal side which needs to be digitally signed. Bidder needs to note that digital signature file will be provided by OICL however the

deployment of the same and managing the same will be bidder scope. Also, the file needs to be reside in HSM and all the policy document generated needs to be digitally signed before sending the policy document to customer.

2.6.1.31 API gateway

In today's scenario financial industry is moving towards linking to online channel and linking those channels with different merchants and provide a better experience of digitization to their customers and promoting online shopping and booking. Bidder needs to fulfill all the compliance mentioned in Annexure 15 - Functional & Technical Specifications.

The bidder is also required to supply, size, implement and maintain the server hardware, Storage, OS, Databases and required to install the API Gateway at cloud.

Bidder need to procure, implement, maintain the required server hardware, Storage, OS and Databases for the tools. Any other software & hardware required by the bidder for API Gateway needs to be procured and implemented by the bidder. Bidder needs to fulfill all the compliance mentioned in Annexure 15 - Functional & Technical Specifications. Bidder needs to provide API gateway as the service in the cloud

All the merchants whether its hotel, railways, airplane, restaurants etc are now a days moving towards digitization and online baking which is good source of revenue to Financial Industry also if they can provide faster and reliable online service.

The key factor to acquire this online business is how fast a Financial Industry can onward a merchant which can only be possible through managing and re-using the API services in the structure way.

There are different statutory initiatives which also mandate Financial Industry to have an API service like Central KYC, Direct ADF – MIS for IRDAI etc.

As the online interaction increase more and more API needs to be exposed from the Financial Industry environment to outside world which also require to be secure and encrypted.

Bidder needs to design, supply, size, maintain install and commission an on Cloud API gateway which will be a single communication channel for all the Third part API which will be getting expose from Portal & Mobile app. Bidder needs to factor all the cost of the same in the bill of material. The API gateway proposed by the bidder should be complied with the below mentioned features as well as the technical requirement mentioned in the RFP

1. Onboard new merchants quickly which will help in increase revenue
2. Provide more secure and encrypted environment to have seamless transactions
3. Increase customer experience

4. Comply with Statutory required more quickly and efficiently.

5. Provide a holistic view of all the API which are going out and coming in which their effective usage and more control manner

2.6.1.32 ADR

To manage the Disaster Recovery Operations more efficiently, OICL is planning to implement an ADR solution for **Mobile app and Portal applications**.

The Bidder is required to design, supply, install, train, customize, test, implement, rollout and maintain the ADR solution and hardware at cloud as per the requirements of this RFP. Bidder needs to fulfill all the compliance mentioned in Annexure 15 - Functional & Technical Specifications. The bidder is also required to supply, size, implement and maintain the server hardware, Storage, OS, Databases and required to install the ADR Tool. Bidder needs to provide ADR as a service in the cloud

Bidder need to procure, implement, maintain the required server hardware, Storage, OS and Databases for the tools. Any other software & hardware required by the bidder for ADR tools needs to be procured and implemented by the bidder. Bidder needs to fulfill all the compliance mentioned in Annexure 15 - Functional & Technical Specifications. The Bidder is expected to provide and implement an ADR solution encompassing the following functions:

1. Align the DR Management to meet the client's business objectives.

2. Provide an efficient, rationalized and integrated Automated DR solution.

3. Maintain the desired RPO and RTO for applications and IT Infrastructure

4. Continuously improve efficiency of DR Drill.

The Disaster Recovery Management Solution should be a single integrated business solution covering all functionality and flexibility required to carry out the Disaster Recovery operations in the current and foreseeable future. It should support all kinds of monitoring that are involved in a DR environment and also should be able to perform DR Drills in a complex environment. It should be a ready to deploy solution with pre-defined templates, and not merely a framework, to support a green field operation. It should provide a competitive edge to the OICL, especially with respect to offering innovative OICL products with a quick time to operational efficiency, operational controls, superior service delivery, better risk management, higher experts retention, highest levels of regulatory and internal policy compliance and timely management information to support quick decision making at all levels of the OICL. OICL is looking out for a comprehensive DR Management Solution for its Core Insurance Applications, Mobile app and Portal.

1. The high-level scope of work for the Bidder is to provide the following services:

2. Design, Size, Supply, Implement and Maintain the Automated DR Solution including hardware, OS, database etc.
3. At least first 4 DR drills to be conducted by OEM after successful implementation of proposed solution and training to be given to the OICL's staff. Subsequently all DR Drill to be performed by bidder
4. Any Change management process or upgrade process in Software should not affect the production database or application. No changes should be prescribed in the database or replication.
5. The offered solution shall have workflow-based monitoring, management, troubleshooting features.
6. The offered solution should have reporting capability for the real time monitoring of a DR solution parameters like RPO (at DB level), RTO, and replication status and should provide alerts (including SMS and e-mail alerts) on any deviations.
7. The proposed solution must support all major platforms including Linux, Windows, Solaris, HP-UX, and AIX with native high availability options. It must support both physical and virtual platforms.
8. The proposed solution must have pre-packaged support for all widely used databases like Oracle, MSSQL, MYSQL, Sybase, PostGre SQL, DB2, NoSQL etc. It must support both physical and virtual platforms.
9. The proposed solution should integrate seamlessly with the existing setup without the need to reconfigure or remove existing application setup including clusters.
10. The offered solution should integrate with AAA (Authentication, Authorization and Accounting) systems like Active Directory / LDAP or equivalent.
11. The offered solution Solutions should be compatible with database log-based replication and transaction-based replication.

2.6.1.33 APM

The bidder is required to design, size, supply, implement and maintain application performance management and assurance tools for **Mobile app and Portal**. Bidder needs to fulfill all the compliance mentioned in Annexure 15 - Functional & Technical Specifications. The bidder is also required to supply, size, implement and maintain the server hardware, Storage, OS, Databases and required to install the APM Tool on cloud.

Bidder need to procure, implement, maintain the required server hardware, Storage, OS and Databases for the tools. Any other software & hardware required by the bidder for APM tools needs

to be procured and implemented by the bidder. Bidder needs to fulfill all the compliance mentioned in Annexure 15 - Functional & Technical Specifications. Bidder needs to provide APM as the service in the cloud

The scope of the application performance management and assurance services should include, but not limited, to the following:

1. Bidder is required to do design, size, supply of software and hardware, implementation, monitor and manage the proposed APM Tool.
2. Bidder is required to Preventive monitoring of mentioned Applications
3. In the event of a critical Alert application experts would step in to carry out initial analysis and hand over the observations for the respective teams to action the same to prevent the event from happening.
4. Provide suggestive restoration / preventive advises as applicable to ensure stability of the environment
5. APM should minimize the application downtime and provide visibility on batch operations.
6. The APM and assurance services should provide the capability to have a deep dive analysis of infra (Web, App, DB, OS & Storage) component even post alert and reduce the MTTR on issues faced.
7. APM application should be cloud agnostic and can be deployed on other cloud (CSP) if required.
8. APM has to provide alerts immediately via, Email to the designated person at OICL end in case of any event occurs in application which may cause the issue on its usage, performance, scale, security etc.
9. Install the APM Agent/s and associated configuration through scripts
10. Deploy new features and fixes seamlessly and automatically into the product as per schedule
11. Create scripts/configure APM Software to scale the Management Cluster with no or minimal configuration and no dependencies on third party software
12. Configure the System for High Availability
13. Perform version updates without downtime for all the component such Reporting Server plus agents etc
14. Cross-datacenter high availability for the cloud installations with near zero RPO / RTO.
15. The automatic notification should be configured in the system and send to designated Email-ID by the application.

16. The proposed solution should provide support for any http, https or non-http applications and should have the ability to add environment specific custom KPI's.

2.6.1.34 AI enabled Chat Bot / Voice Bot

Bidder needs to propose the AI enabled Chatbot for the Corporate Portal of the OICL. Bidder needs to factor all the commercial in the bill of material of the contract duration. Bidder needs to factor all the cost of installation, commission and integration of the same. Bidder also needs to factor all the hardware and software required for the same in the cloud. **Bidder needs to fulfill all the compliance mentioned in Annexure 15 - Functional & Technical Specifications.**

Bidder need to procure, implement, maintain the required server hardware, Storage, OS and Databases for the tools. Any other software & hardware required by the bidder for Chatbot needs to be procured and implemented by the bidder. Bidder needs to fulfill all the compliance mentioned in Annexure 15 - Functional & Technical Specifications

Humans are always fascinated with self-operating devices and today, it is "Chatbots" which are becoming more human-like and are automated. The combination of immediate response and constant connectivity makes them an enticing way to communicate and get their queries resolved.

From retail client to apply for policy, claims, other products to reporting fraudulent activity, financial consumers think digital first. With Chatbot OICL is looking a chatbot as first point of integration for fulfilling the digital needs of customer engagement technology that will help build revenue, drive satisfaction and retention, and lower servicing costs.

With unique blends of Artificial Intelligence, Deep Learning Modules and Natural Language Processing (NLP) capabilities Chatbot platform Should have below:

Omni-Channel Communication: Chat clients over Website, Mobile, Social Media (WhatsApp, Facebook Messenger, Instagram, Twitter, WeChat, etc), Phone Call (IVR Integration), Smart Devices (Alexa, Google Home Assistant)

Conversational AI: Chat with BOT like with Human. Engine Works on Intent Classification of user message through NLP

Speech-To-Text & Text-To-Speech: Capabilities like Automatic Speech Recognition (ASR), it transcripts the user voice into text and process the query for replying to user with BOT voice response through Text-To-Speech

Live Human Agent Support: Humans and BOT works together to provide excellence in customer support. User can directly chat with Human on the same chat client whenever he wishes to or if the BOT is not able to assist the user it will automatically transfer the chat or call to Live agent for further support

API Integrations: Integrate the chatbot with any third-party application like CRM, ERP, and any other information/data source

Chat Analytics: Platform should provides sentiments-based chat analytics which is useful to predict user behavior in terms of Happy, Sad or Anger.

Auto Filling of Form: - Chatbot should have the ability to convert the speech to fill the form automatically.

Integration:- Chatbot needs to integrated with Handheld device like Pos and other devices based on the SRS.

2.6.1.35 Password Less Authentication

OICL is looking to introduce a new feature to ensure more safety and digital mechanism to login into the portal without password. Bidder needs to factor all the cost and required License and implementation and integration cost in the bill of material. The solution proposed by the bidder must be complied with Annexure 15 - Functional & Technical Specifications. Bidder needs to factor the Lic as per the customer projection mentioned in the RFP.

The bidder is also required to supply, size, implement and maintain the server hardware, Storage, OS, Databases and required to install the Password Less Authentication. Bidder needs to install the solution in the cloud infrastructure

Bidder need to procure, implement, maintain the required server hardware, Storage, OS and Databases for the tools. Any other software & hardware required by the bidder for Password Less Authentication needs to be procured and implemented by the bidder. Bidder needs to fulfill all the compliance mentioned in Annexure 15 - Functional & Technical Specifications

The proposed software should be able to do the following

1. Integrate with multiple channels like whats app, SMS, IVR, SIEM etc
2. Ability to have the physical presence test to avoid frauds
3. Provide capability to have the option to using QR code or password as per the customer wish
4. Ability to offer offline authentication methods in an event the user's workstation and/or authenticator does not have network connectivity to the authentication server
5. The proposed Software should have below mentioned Authentication methods
    1) Biometric
    2) OTP
    3) Face recognition
    4) Lively test
    5) OR Code
    6) Password

2.6.1.36 Audit & Governance Requirements

a) The bidder shall implement the audit & compliance features to enable OICL or its nominated agency to monitor the provisioned resources, performance, resource utilization, and security compliance:

b) View into the performance and availability of the cloud services being used, as well as alerts that are automatically triggered by changes in the health of those services.

c) Event-based alerts, to provide proactive notifications of scheduled activities, such as any changes to the infrastructure powering the cloud resources.

d) System-wide visibility into resource utilization, application performance, and operational health through proactive monitoring (collect and track metrics, collect and monitor log files, and set alarms) of the cloud resources.

e) Review of auto-scaling rules and limits.

f) Logs of all user activity within an account. The recorded information should include the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the cloud service. This is required to enable security analysis, resource change tracking, and compliance auditing.

g) Ability to discover all of the provisioned resources and view the configuration of each. Notifications should be triggered each time a configuration changes, and Department or its nominated Agencies should be given the ability to dig into the configuration history to perform incident analysis.

h) Monitoring of cloud resources with alerts to customers on security configuration gaps such as overly permissive access to certain compute instance ports and storage buckets, minimal use of role segregation using Identity and Access Management (IAM), and weak password policies.

i) Automated security assessment service that helps improve the security and compliance of applications deployed on cloud by automatically assessing applications for vulnerabilities or deviations from best practices. After performing an assessment, the tools should produce a detailed list of security findings prioritized by level of severity

2.6.1.37 Quality Assurance & Audit

The OICL will require the Bidder to establish and maintain an effective quality assurance program to ensure the technical quality of all products and services provided under any task is in order. This will include, but not be limited to, Portal solution quality monitoring, methods to identify and correct quality deficiencies in products and services and methods for continuous improvement. Quality Assurance activities include development of quality assurance plans and procedures; collection and reporting of metrics, define project-specific metrics; conduct reviews; participation in any OICL – conducted reviews, walkthroughs, or other required meetings held throughout the Portal development life cycle; and development of responses to the results of any OICL Portal quality assurance activity.

The bidder should arrange to conduct periodic risk management analysis, security vulnerability assessment of the portal application at least once in a year.

The websites would also be periodically audited by OICL appointed auditors. The audit scope can include source code, vulnerability assessment, and penetration test of related infrastructure. The successful bidder will facilitate audits; fix/rectify all the vulnerabilities reported by the security auditors without any cost to OICL and within 30 days of getting the reports.

The solution provider shall ensure adherence to Guidelines for Government Websites including mandatory “Safe-to-host" certification. It would be the responsibility of the selected bidder to get Safe to Host certificate for the portal from the Cert-In empaneled vendors and to remove the vulnerabilities identified during the Safe to Host certification. Bidder shall submit the Safe to Host certificate for the developed website before go-live

2.6.1.38 3rd party Audit Certification

The SI will be responsible for engaging a reputed 3rd Party to conduct the assessment / review for the system before “Go Live”. SI shall ensure the following points are duly addressed for successful completion of 3rd party Certification. Successful completion of Application Audit. Application audit will include: -

3. Functionality audit that will map the functionality delivered to the SRS agreed upon during implementation phase.
4. Identify the nature and type of transactions being processed by the application systems.
5. Determine systematic measures implemented to control and secure access to the application programs and data including password controls, user authentications, roles and responsibilities, audit trails and reporting, configuration and interface controls, etc.
6. Review of database structure including:

- Classification of data in terms of sensitivity & levels of access
- Security measures over database installation, password policies and user roles and privileges
- Access control on database objects – tables, views, triggers, synonyms, etc.
- Database restoration and recoverability
- Audit trails configuration and monitoring process
- Network connections to database

7. Review of Network and Website will include:
8. Penetration and vulnerability testing
9. Security exposures to internal and external stakeholders

2.6.1.27 Hardware

Bidder is required to size, supply, design, commission and maintain hardware, OS, DB as well as all software required for the proposed applications that should be as per the contract duration mentioned in RFP document for all environments, i.e. DC, DR and Non-Production (Test, Development, UAT, pre-prod & Training). The bidder is required to host all the environment of Portal Mobile app and other tools asked in the RFP on cloud.

Bidder needs to provide all the details of each components (server, storage, space, middleware, SAN Switch, Tor Switch, or any other component required as part of the solution) like make, model, configuration, architecture etc.

Bidder should consider high availability at all three layers for Portal and mobile app. Weblayer and Application layer should be load balanced in Active- Active at DC and DRC and database layer can be proposed in active-passive. The architecture at disaster recovery centre should be a 100% replica of primary data center.

The hardware details must include:

Server and Storage (usable capacity and RAID) requirement

Production Environment (Web, Application, Database, Middleware etc.) at DC and DRC

All Non - prod (Test & Development, UAT, Training and Pre prod) Environment at DC

For all the Tools (APM, ADR, Chatbot, password less Authentication, API Gateway, HSM, KSM) only one non-Production needs to be factor at DC location in cloud. Bidder Needs to Factor HA environment in DC and standalone environment at DR for Tools (APM, ADR, Chatbot, password less Authentication, API Gateway, HSM, KSM)

The bidder shall Design, size, supply, maintain hardware 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. Bidder is required to submit **Annexure 18- sizing adequacy letter** mentioned in the RFP.

Bidder will have to deploy hardware resources at DC and DR as per the project plan on the proposed cloud. Hardware technology proposed by the bidder should be based on the latest offerings by the respective OEMs.

a) The hardware should be of enterprise class, best of breed, tested and stable release of OEM.

b) Vertical and horizontal scalability should be two important requirements for these cloud deployment and application development.

c) Cloud Storage should be able to create space efficient clones for the Production Volume. Clones should consume space only for the changed data.

d) Cloud Storage should also support Storage Efficiency Features like Thin Provisioning, Deduplication and Compression to reduce the Primary Storage capacity requirement.

e) Cloud Storage should support backup on low-cost Object storage. All the storage efficiency benefits should be available on Object storage also to reduce secondary storage requirement.

f) Cloud Storage should have the flexibility to move data from one Public cloud to other Public clouds seamlessly.

g) The database server storage has to be provided on high speed disks (SSD's) for better performance

Bidder should arrive at the sizing independently keeping growth roadmap in consideration. Also, during the contract period, growth of the OICL should be considered and thus, the hardware proposed should have enough CPUs, memory and storage available to accommodate the predicted sizing required.

All hardware (required for interface, staging, Web Server, development and training server, and related hardware components) and system software components required for the project, must be included in the bill of Material of the Bidder. In case, Bidder fails to do so and the project demands additional components at a later stage, then Bidder will have to provide additional components at no additional cost to the OICL. DB audit trail should be enabled across all environments and bidder is required to size the hardware accordingly.

As per the architecture there are 5 copies of databases required at DC. Prod, test & Dev, Training, UAT & Pre prod with a performance neutral volume clones for each of the workloads and a full volume copy. These copies shall have incremental updates. Taking of backup for the onsite tools proposed in the RFP will the responsibility of the bidder and bidder needs to factor necessary equipment and cost for the same.

Bidder can consider Logical separation/ Virtualization for production and non-production environment at compute and storage level for respective Environments.

The bidder should note that the production and non-production environment should be physically separate with respect to Compute.

The Pre-Prod servers sized should be minimum 25% of the size of the production as per the fifth-year sizing however the database size will be similar to production database size.

The Test, Development, UAT & Training servers should be minimum of 10% respectively of the size of the production as per the fifth-year sizing however the database size will be similar to production database size

The Bidder can propose the latest version of industry leading RDBMS software.

Bidder is required to perform the following activities other than the ones called out as part of Responsibility Matrix below:

1. Installation/ Creation/ Re-Installation of databases with suitable hardening procedures as per OICL's policy.
2. Fine tune and resolve performance issues through performance tuning and optimizations.
3. Provides the required operational support to monitor the proposed applications database environments
4. Refers to the successful backup and restoration of the database instances as defined by OICL policy
5. Management of the granting, removal, monitoring and editing of access rights allocated to the database and application environments based on the OICL's direction and approval
6. Processes to perform database upgrades, performance tuning and repairing a database (if required)
7. Create, Implement and validate database recovery solutions. Support during DR testing and during actual DR situations

2.6.1.28 DR Setup

1. Bidder has to ensure that DR setup is ready on the date of Go Live of solution
2. Bidder should make necessary setup to enable the DR within the agreed timelines.
3. Bidder should carry out the deployment of the application in DC and DR, UAT as applicable.
4. To ensure proper rollback, bidder has to ensure that the old setup at all the locations is As –IS as per the agreed timelines during migration strategy formulation.
5. DC and DR to be on cloud
6. To achieve complete replication of data and maintaining one copy of data on DR site, the storage shall be replicated 100% and shall be sized accordingly to maintain the data at DR site
7. Providing N/w components at DR site shall be in scope of the bidder and it shall be responsibility of Bidder to ensure network configuration at DR similar to that of DC site

8. Providing Security components at DR site as per Department requirements shall be in scope of the Bidder and it shall be responsibility of Bidder to ensure configuration at DR similar to that of DC site though the Department may choose security components to be in standalone mode in DR

9. DR Site would be Hot or warm Disaster recovery Site

10. Disaster Recovery resources are configured at 100% of Production Data Centre capacity.

11. All Application, Database, Stateless and IT infrastructure servers are replicated to DR site and are operational at all the time.

12. Recovery point operation is High/Aggressive (near zero to Minimal data loss)

13. Recovery time operations to be near zero using Multi-Cloud Global Server Load Balancing (GSLB)

2.6.1.29 Software

The following considerations must be taken for supply of software:

- All software envisaged is required to be licensed to OICL.
- The software supplied must be the latest version of the software supplied by the OEM.
- Beta versions of any software shall not be accepted.
- The bidder shall ensure that the software licenses supplied in its bid adequately cover the needs as per the requirements in this RFP.
- The bidder must consider the disaster recovery environment while proposing the software licenses.
- The successful bidder should provide comprehensive ATS for proposed solution, including other software, associated modules and services required to meet the requirements in the RFP.
- The support for the solution should include the following:
  - All minor version upgrades during the period of contract at no extra cost to the OICL
  - Program updates, patches, fixes and critical security alerts as required
  - Documentation updates
- The proposed Application version should not become End of Support for the entire contract duration.

2.6.1.30 External Agency for UAT and Data Migration Audit

Testing: -

Bidder has to engage an external testing agency during the implementation stages. The external testing agency and bidder will completely be responsible for end-to-end UAT and data migration audit.

Data testing on pre & post migration state of data is part of the scope. Testing agency will have to report on field level variances, if any.

Based on the contents of the RFP, the testing agency will be required to arrive at Test Methodology in consultation with the OICL, based on a standard which is suitable for the OICL and perform UAT on behalf of the OICL. The external testing agency will completely be responsible for end-to-end UAT.

Vulnerability Assessment Penetration Testing (VAPT) to be conducted quarterly or as specified by the regulatory authority/ OICL is also part of the scope of the CERT-IN empaneled testing agency.

Information Security Audit to be conducted quarterly or as specified by the regulatory authority/ OICL is also part of the scope of the CERT-IN empaneled testing agency. However, the testing agency has to ensure that the IS Audit is conducted before the Go-Live and all observations are closed.

Bidder needs to note that training need is to be conducted by the bidder manually.

External Agency will be responsible for performing the below activities:

1. Development of suitable testing methodology/testing strategy document
2. Development of test cases in consultation with the OICL. Bidder has to provide already prepared test cases to OICL (not less than 500, negative & Positive) which OICL may approve/ modify before execution.
3. Development of test calendars.
4. Execution of all the test cases.
5. Development of entry and exit criteria for testing.
6. Development of detailed test scripts in UAT environment.
7. Test application software for functionality, operational convenience, security and controls. This will also include positive and negative cases for each type.
8. Testing will be done on LAN as well as WAN environment including HO, RO, internet and Branches, as desired by the OICL.
9. Point out gaps, errors, bugs during testing.
10. Document the gaps, errors and bugs observed during testing.
11. Maintain a track of errors, bugs and customization requests and their resolutions'.
12. Explain bugs, errors and gaps to the OICL and application vendors.
13. Follow up with Application vendor for fix or patch.
14. Re-test the gaps, errors and bugs after rectification.

15. Assist in Sign – off on the customization
16. Assist in Sign – off on user acceptance test.
17. Submit all documents on methodology, strategy, test cases, test documentation, customization requests, solution etc. to the OICL.
18. External testing agency and the bidder together will be responsible for end-to-end testing and UAT activities within scheduled timelines.
19. Testing must include test cases on calculation and application of charges, EOD / BOD, premium calculation, batch job execution, month end / half year end and yearly EOD / BOD, Claim generation response time etc.
20. All testings will be carried out with resources provided by the External agency in coordination with the OICL.
21. Acceptance testing shall broadly cover the testing of functionalities, migrated data (pre and post migration), and all interfaces to verify that the proposed solution conforms to the business & technical requirements and Gap analysis Report, Bandwidth and response time.
22. Bidder must fix the bugs, carry out necessary rectifications and deliver patches/version towards changes which would be reported by external agency and the OICL.
23. Bidder/ 3rd party testing agency is required to factor in mobile devices and all other required devices of various form factors for testing of solution.
24. OICL shall accept the application software only after critical or major Bugs are fixed and are ready for production Implementation.
25. Record test results against the test cases tested.

- The testing should also ensure conformity to:
- All customized menus and reports are working as per expectations.
- All customized Interfaces are working as per expectations.
- All functionalities are working properly as per the SRS document provided by the Bidder.
- Gaps identified
- Interface testing with all types of transactions pertaining to that interface.

Data Migration Audit

Bidder shall be required to engage a third party to recommend the audit methodology and tools, which is suitable for OICL and audit the Data Migration as per timelines of the project implementation. The external testing agency will completely responsible for end-to-end UAT and data migration audit.

Bidder has to carry out Data Migration Audit based on the recommended audit methodology.

The Bidder shall perform the following audit checks:

Data integrity checks: Pre-migration and post-migration data sets should be compared for data integrity issues. Data integrity checks should check the following data parameters:

1. Raw data integrity
2. Business rules
3. Log Tables
4. Configuration/ Parameterization table

To ensure that the data in the new migrated environment qualifies the integrity and reliability tests and in case any errors or mistakes are identified, suitable counter measures are taken by Migration team for mitigating their impact.

1. Identify the critical fields (upto 100) to be validated from the field in source system based on the experience of other migrations.
2. Business rules verification.
3. 100% of Configuration/parameterization table should be verified.
4. Vendor is expected to verify log tables and highlight various error logs if any, post migration.
5. To provide an assurance that 100% data for critical fields has been properly identified and accurately and completely migrated to relevant data fields in the target system by understanding and validating the migration controls, performing independent verification of Data migrations
6. Review back-up procedure so as to ensure SI will provide assurance of availability of data under conversion ensuring that and not limited to that the data is backed up before migration for future reference or any emergency that may arise out of data migration process.
7. Assessment of reliability of the financial data/ other critical data files
8. Comparison of pre-migration and post-migration data for checking integrity issues.

Deliverables of data migration audit

1. Data migration audit strategy.

2. Migration process review report

3. Field wise Exceptions reports (pre & post)

4. Final compliance report, post migration.

External testing agency and the bidder will be responsible for end-to-end UAT and Data Migration audit activities. Bidder needs to note that the external Agency quoted for doing UAT and Data Migration UAT needs to deploy a dedicated Project Manager onsite for Managing the UAT and Data Migration UAT

2.6.1.31 Project Management

Project Management activities will be carried out by bidder with support from the OICL as required. The Project Management Office will address the overall allocation of work packages and direct co-ordination of activities and portfolio governance.

The Bidder should follow an industry standard Project Management methodology which has been agreed with the OICL.

The Successful Bidder shall develop and implement a governance mechanism to institutionalize and effective approach towards planning and organizing, acquiring and implementing, delivering and supporting and monitoring service performance of the services deployed in OICL to support its business requirements and objectives.

Principles of Governance

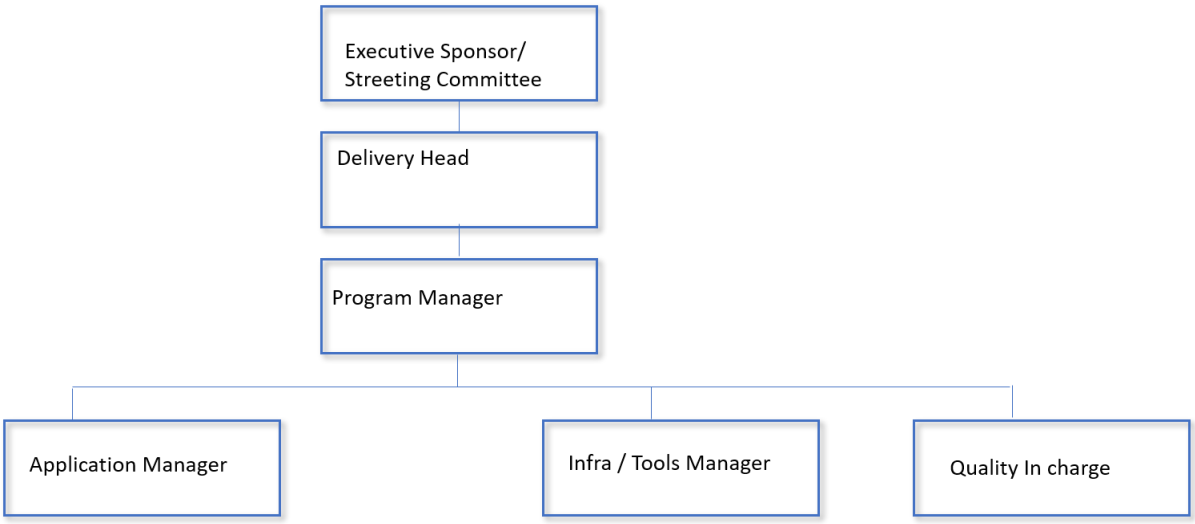
For managing the operations effectively and meeting the contractual requirements and SLAs, OICL proposes to set-up governance mechanism with following principles. The Bidder will assist OICL by adhering to the below principles:

- Bringing focus and discipline in governance mechanism.
- Setting clear policies and procedures.
- Strengthening ethics and accountability.
- Continuous vigilance and adaptation.
- Strong financial oversight.
- Independent audits to bring more objectivity.
- Strong quality checks

Indicative structure of governance set-up

The Successful Bidder is required to develop the framework and capacity for making and implementing decisions required to manage and control IT Infrastructure and services monitoring and management within the business. IT Governance scope shall encompass the structures, processes, responsibilities, decisions for operation of IT Infrastructure and services monitoring and management. The Successful Bidder shall be provided with OICL's existing Policies/procedures/SOPs etc. which can be used to develop governance and Quality framework for IT services management in OICL.

The Successful Bidder should propose an organization structure with regard to governance of the Contract. An indicative organization structure is outlined below:



Please note that this is an indicative organization structure. The Successful Bidder has to provide the details as per deployment chart, as per the format specified in the Annexure 19- Project Team Profile.

Governance Structure

Governance Layer	Governance Participants		Responsibility	Review Frequency
	OICL	**Service provider**		
Steering Committee	General Manager, DGM IT,	Executive Sponsor	1. Define strategic objectives 2. Ensure continual executive 3. Performance reporting 4. Issue resolution (Final escalation level)	Quarterly/ Semi Annually

Program Management	Chief Manager -IT	Program Manager	1. Account Management 2. Monitor service delivery • Single point of contact for issue escalation 3. Issue resolution (Intermediate escalation)	Monthly
Operations Management	Operations Managers / supervisor	Manager s	1. Issue resolution and escalation 2. Manage people issues 3. Plan, track and review SLAs 4. Plan and track timelines	Weekly Monthly Quarterl y
Project Manager-Tools	Lead for Tools Implementati on	Project Manager Tools	1. Single point of contact for issue escalation 2. Issue resolution (Intermediate escalation) 3. Plan, track and review SLAs 4. Plan and track timelines	Ad-hoc Weekly Monthly Quarterl y

Performance management and reporting

The Successful Bidder shall be required to report on the services offered to OICL on a periodic basis or as and when required by OICL. The Successful Bidder shall provide reports/ data that would include but not be limited to:

1. Performance report with respect to all service levels.
2. Report of the ongoing and planned changes performed.
3. Any ad-hoc report that may be required by OICL
4. Periodic reports to governance committees; and
5. Quality adherence reports

These reports would compare the quality of service provided with the defined/target SLAs. The list of reports and their frequency should be agreed with OICL in the start of the Project.

During transition, reporting and review of performance metrics shall be carried at mutually agreed frequency (to be decided along with Service Provider).

The template and any other reporting requirement shall be agreed on mutually. In addition, the Successful Bidder will provide assistance to OICL for audit/compliance related requirements, including but not limited to:

1. Providing sample data as required within the timeline; and
2. Coordinating with other sites for providing data samples.

The ownership of audit/compliance related requirements shall remain with OICL.

Quality Assurance

Scope related to Quality Assurance (QA) shall include:

1. Developing and employing a quality assurance program, subject to OICL approval, designed to promote performance of the scope of work with a high level of quality, focusing on measuring and improving reliability, speed, cost effectiveness, and customer satisfaction.
2. Writing and maintaining procedures and measurements on all quality assurance activities associated with the work. Ensuring that the quality metrics and procedures employed are consistent with similar standards in OICL's peer group and/or in the provision of similar professional services.
3. Ensuring compliance with a published quality assurance program, with adequate internal controls and verification activities.
4. Conducting periodic quality audits of the work rendered.

Documenting audit findings and remediating non conformances within a stipulated time period. Allowing OICL to perform audits that will focus on the Successful Bidder's adherence to its quality assurance procedures and standards; on the metrics gathered to support quality assurance activities; and on the Successful Bidder's efforts to improve overall quality. The Successful Bidder will cooperate fully and assist OICL with any such audits.

Service Window across Service Category

Domain Management	
Server Management Services	24 x 7 x 365
Storage Management Services	24 x 7 x 365
Database Management Services	24 x 7 x 365
Backup, restore & Archival Management Services	24 x 7 x 365
Cross Functional Services	
Performance management & reporting	24 x 7 x 365
Incident Management & Application Monitoring Group Support Services (IT Infrastructure)	24 x 7 x 365
Change & Release Management	24 x 7 x 365

Service Level Management	24 x 7 x 365
Security Management	24 x 7 x 365
Software Distribution	24 x 7 x 365
Software License Management	8 x 6
Vendor Performance Management	8 x 6
IT Continuity and Disaster Management	24 x 7 x 365
APM, API Gateway, ADR, HSM, KSM, Password less Authentication	
APM, API Gateway, ADR	24 x 7 x 365

2.6.1.32 Minimum Resource On-site Deployment during implementation phase

Bidder shall at minimum deploy the resources as per the minimum deployment level mentioned below during the Implementation Phase. Bidder should independently arrive at the sizing and deployment plan to meet the RFP requirements (As per scope of work and SLAs) adhering the minimum deployment level during the implementation stage. Bidder shall deploy resources at no extra cost if the proposed deployment does not meet the RFP requirements and SLAs.

Bidder needs to ensure that there should be atleast 2 PMO resources which are factored for the Implementation stage which will be involved in the Project management of the overall Project and should be from Independent Third Party. Bidder needs to note that these PMO resources must have knowledge of the managing the Turkey Project and must have experience of more than 10 years.

Bidder needs to ensure that there should be atleast 2 SME Resources which are factored for Implementation stage which will be doing the requirement gathering and will be server as a bridge between business team of OICL and Development team of System Integrator. The proposed SME resources should have below mentioned experience

1. Minimum 8 years of experience in General Insurance Sector
2. Should have worked as Business Analyst and experience of written SRS and doing requirement gathering for atleast 4 years

OEM's involvement for onsite implementation effort being proposed by the bidder during the implementation should be 20% of the overall effort of respective components (API gateway, ADR, APM, Chatbot) and the same shall be factored in the Bill of Material. During the course of implementation OEM involvement should be spanning across all phases of implementation including Project Preparation, Solution Design Phase (Including Review/design of all the Documents,

HLDs/LLDs/ Blueprints and other Solution documents), Migration (if applicable, Configuration and Customization, Integration, Acceptance and Training).

Resource	Location	Minimum Number of Resources	Total Number of Resources
Program Manager	OICL Corporate Office	1	1
Infra In charge	DC	1	1
Database In charge	DC	1	1
New Tools In charge	DC	1	1
Application In charge	OICL Corporate Office	1	1
DR In charge	DR	1	1
PMO Resources	OICL Corporate Office	2	1
SME Resources	OICL Corporate Office	2	1

The Successful Bidder should propose an organization structure with regard to governance of the Contract. An indicative organization structure is outlined below:

As part of the project management exercise, the bidder is expected to:

1. Setup the project management office and framework comprising of:

- Project charter formulation
- Project risk analysis
- Assistance in project management and project delivery team identification and resourcing
- Change management procedures
- Project planning and detailing
- Project quality management procedures
- Employ a formal project methodology on all projects undertaken with the level of detail and control scaled appropriately to the magnitude of the project effort and adhere to all project management processes and procedures

2. Project Manage the following phases of the project:

- Current State assessment
- Business parameterization

- Gap analysis and Customization
- User Acceptance testing
- Data migration
- Rollout

3. Closure of issues pending for resolution
4. Measure the progress made in the implementation of the project
5. Track customization and gaps
6. Monitor closure of gaps and customizations as per delivery schedules
7. Provide regular updates to the steering committee and board as required by the OICL.
8. Participate in all technical and functional discussions relating to the projects
9. The bidder is required to project manage the Go-Live and provide executive reports.

2.6.1.33 Training

Bidder is required to provide user training to optimal number of personnel identified by OICL on functional and technical operational aspects of the applications and in scope.

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.

S.No.	Training Type	No. of days per batch (Working days)	No. of batches	No. of trainees per batch
1	Portal training	15	1	10
2	Mobile App	15	1	10
3	Core Team Training- Technical & Administrative for Mobile and Portal	15	1	10
4	API Gateway Training	3	1	10
5	Chatbot	3	1	10
6	ADR	3	1	10
7	APM	3	1	10
8	Portal And app code-based training	5	1	10
9	HSM, KSM	3	1	10

On receipt of each deliverable, OICL will review each deliverable within agreed time frame. It is also the responsibility of OICL to identify and ensure attendance of appropriate personnel.

2.6.1.34 Go-Live

1. Bidder has to provision for adequate no. of resources and ensure that they are well-versed with OICL's specific solution functionalities, integration and customizations throughout the contract period.
2. Go-live shall be considered as complete when the respective application usage is tested and signed off by OICL.

2.6.2 Phase – 2 - Facilities Management and AMC/ ATS

This section of the On-Going Operations is broadly classified under Two (2) categories of services that the Bidder is required to offer.

1) Domain Services
2) Cross Functional Services
3) Application Management

Any other tools required by the Bidder for offer the services as per the RFP should be proposed and factored in the bill of material.

2.6.2.1 Domain Services

OICL has identified number of domain services to support business operations. Bidder is expected to provide support for these domain services as per the defined scope and the corresponding SLAs.

The following table presents an overview of the services to be provided by Bidder under domain services, on an ongoing basis for the duration of the contract. Bidder is expected to adhere to IT Service Management (ITSM) processes based on IT Infrastructure Library (ITILv3) framework (version 3) for all the services:

Domain Services	Description
Database Management	The management of the provisioning, maintenance and support of database hardware and software as well as monitoring, access management, backup and recovery and ad hoc support
Server Management Services	Monitoring and management of computing platforms on which utilities and applications are hosted
Storage Management Services	Monitoring and management of the enterprise storage environments within OICL. This also includes storage area networks (SANs) Replication and storage on distributed file

Backup and Restore Management Services	Management of backup facilities of OICL of in scope explanation, including the mechanics of D2D Backup, tape backup, such as storage management, tape collection for off-site storage, handover of tapes to OICL's resources for offsite tape storage and retrieval of tapes from OICL's resources in the event that restoration of historical data is required. The Successful Bidder shall be responsible for taking centralized backups from DC and DR for all the servers hosted at DC, DR.

2.6.2.1.1 Database management

The scope of the database management services includes all data and database management of in scope applications (Oracle, Sql etc) activities on the production, non-production and disaster recovery environment that will be included as part of this service. The expected database management services can be further defined by the following high-level service requirements:

Domain Services	Description
Build, Installation	Definition/ Installation/ Creation of databases with suitable hardening procedures as per OICL's policy
Database Performance Management	Fine tune and resolve performance issues through performance tuning and optimizations.
Database Capacity Management	Estimate & recommend database requirements based on performance and Business projections
Monitoring and administration	Provides the required operational support to monitor OICL database environments
Backup and restore	Refers to the successful backup and restoration of the database instances as defined by OICL policy
Access management	Management of the granting, removal, monitoring and editing of access rights allocated to the database environments
Database ad hoc support	Processes to perform database upgrades, performance tuning and repairing a database
DC and DR testing	Create, Implement and validate database recovery solutions. Support during DR testing and during actual DR situations

General

1. The scope of work mentioned is illustrative and not exhaustive. The bidder needs to comply with OICL's requirements and any statutory or regulatory guidelines
2. All oracle and other Database's process and DBMS best practices will be a part of scope

Database Build and Installation

3. Defining the physical database design (log files, rollback segments, tablespaces, database descriptors, partitioned objects)
4. Installation of software and database creation [in consultation with the OICL's team] - Oracle/ SQL etc. as per OICL's standard
5. Create definitions of logical data structures, tables, views, indexes, program specification blocks, stored procedures & define their relationships
6. Hardening process document for fresh DB installation and perform hardening
7. Test and prepare database upgrades.
8. Implement database upgrades into the production, non- production and DR environments
9. Publish Plan of Action (PoA) to be verified and validated by OICL's team before implementation

Database Performance Management

10. Track & co-ordinate database related incidents/ problems till resolution
11. Conduct first level diagnosis for reported Incidents & perform resolution
12. Analysis of incident/ problem trends
13. Co-ordination & escalation to Database vendors (L3) (Logging ticket at Vendor side as well internal tracking through service desk), follow-up till resolution
14. Maintaining & monitoring the health & performance of databases (Primary and standby)
15. Monitor & analyze alerts & logs including
    a. Trace files (including data block corruptions, Enqueue resources, internal errors & I/ O read-write failures)
    b. Database changes
    c. Background job status
    d. Operating system logs
    e. Space management
16. Monitoring the table space utilization, file system usage and all other events of O.S which may deter the performance of the database (primary as well as DR)
17. Analyzing/Troubleshooting Database Performance
18. Collection of statistics for databases
19. Optimizing database performance, Performance tuning
20. Monitor physical DBMS for performance & capacity requirements
21. Monitoring of databases
22. Monitoring of transaction logs
23. Provide recommendations on DBMS design
24. Monitor the backup & report on backup logs
25. DDL, export & import related activities
26. Preparing monthly database related reports
27. Provide databases for MIS purpose on daily, monthly and on need basis
28. Periodic optimization of application databases through compression facilities and database tuning.
29. Provide reports on database currency and propose upgrade recommendations
30. The bidder is required to install & implement database diagnostics & fine-tuning packs based on OICL's requirements.

Database Capacity Management

31. Estimate & recommend database requirements based on received data from Database Performance team and Business projections (Annual/ As and when required)
32. Perform Database Space analysis
33. Alignment to purging policy
34. Review archive logs requirements
35. Customizations required at DB level
36. Review and planning for 6 months

Database Monitoring and Administration

37. Setting data storage parameters for storage associated with the physical elements of the database
38. Handling password issues
39. Configuration of Databases
40. Creating a new database instance
41. Testing & implementation of patches
42. Testing & implementation of upgrades
43. Managing, applying & verifying Database program patches
44. Database Scripting
45. Review recommend and test patches.
46. Coordinate all changes through the agreed upon change management process
47. Start-up and shutdown of databases
48. Daily activities such as end of day, end of month, end of year/quarter etc.
49. Daily / Weekly / Monthly backup of databases
50. Database recovery
51. Weekly database recovery checks
52. Required logs maintenance as per Standards of the OICL
53. Disaster recovery as per Standards of the OICL
54. Database problem resolution
55. Recreation of Indexes
56. Perform pre-batch activities-Scheduling of resources-Scheduling batch services-Define, maintain and document a work schedule for running production system batch jobs, and possible started tasks-Install and document system related batch jobs in the automated job scheduling package-Manage the root cause analysis for scheduling problems- Develop and maintain standards for job acceptance and implementation. The bidder can either use scripts or propose a tool for batch automation
57. Remove applications from the application portfolio following decommissioning from projects or improvements.
58. Perform regular import and loading of data and ad-hoc data extractions.
59. Responsible for maintaining DB inventory
60. Maintaining and performance tuning of UAT databases
61. Migration of Databases (Release Upgrade)
62. Execution of all back-end changes across all applications as informed by application owner
63. Manage database transaction (SQL)/ archive (Oracle) logs
64. Administration/ management of archival databases (Purge from production and move to archive database)

65. Resolving corruption (both Physical & Logical) issues at primary & standby databases
66. Execute DBMS changes in support of major application or logical database design changes
67. Designing &Implementation of logical & physical backups
68. Flash back up on daily basis
69. Vendor coordination with OEMs for upgrades, patches, bug fixes, performance tuning etc.
70. Creation of a Standby database & setting up the DR
71. Using data guard and RAC for Oracle
72. Log shipping/Mirroring/Always On for SQL
73. Monitoring, management and implementation of High Availability (HA) viz. clustering/RAC etc.
74. Review of all databases
75. Switchover of databases (as and when required and as per the defined time window)
76. Refresh of Databases as per defined frequency or on demand
77. Day end, month end, quarter end, year-end End of Day & Begin of Day support
78. Resolution of audit points and VA/PT reports
79. Management of tools
80. Ad-hoc support for processes run by branch charges for average quarterly balance/ SB interest calculation
81. Apply application data fixes.
82. Install patches and upgrades to database software.
83. Installing database software as appropriate.
84. Perform application nonproduction environment data refreshes.
85. Cloning of application data environments.
86. Monitor capacity and performance of databases.
87. Control of the database (adapting database profile parameters, expansion of tables and table spaces)
88. Technical reorganization of the database (defragmentation) also after archiving
89. Analysis of the DB tables & indexes - continual performance enhancement measures
90. Create new indexes, performs reorganizations as required per analysis
91. Creation, maintenance and execution of database related scripts such as start-up and shutdown processes
92. Creating and maintaining formal documentation of the database environment (e.g. scripts, design, configuration, access rights)
93. Monitor availability of the databases as a subset of monitoring overall service availability.
94. Providing solution services for database design, configuration and maintenance
95. Assist with incident and problem management related activities relating to the database environment (e.g. integration, interface, performance, configuration issues as part of the overall support service) including interaction with third party suppliers where necessary.
96. Archive of application specific data as requested.
97. Implementation and monitoring of database security.
98. Loading software components- Kernel patches, Release changes.
99. Proactively apply security fixes
100. Documentation upkeep and records maintenance

Database Backup restore

101. Manage Database backup/ restore schedule, administration (RMAN Backup)/Scheduled Backups and others
102. Data Deletion & Purging/archival activity
103. Purging of tables based on availability of space on a regular frequency (Frequency to be decided)
104. Consolidating all database backups & Transaction log backups at a single file Server
105. Perform database backup, restore and recovery routines.
106. Compliance, review and updates to database standards documents.

Access management

107. Implementing & managing security rules & access authority as per OICL's security policy, database Hardening etc
108. Implementation of database security by creating roles, privileges & profiles
109. Management of users in database and assigning of roles/privileges
110. Monitoring and management of logs for user access management of privileged users

Database adhoc support

111. Provide access to DBA resource for ad hoc work requests and change orders

Database Recovery

112. Create & implement database recovery solutions in consultation with OICL's team
113. Recovery of database at primary and standby as per case
114. Restoration activities (from backup media)
115. Database recovery using the physical & logical backups
116. Support for DR Configuration and BCP activities and Plan
117. Evaluating current backup, recovery, & data replication procedures & providing recommendations for improving those procedures

2.6.2.1.2 Server Management

The scope of the server Management services includes all RISC, EPIC, Wintel and Hyperconverged management activities on the production, non-production and disaster recovery environment that are part of this solution. The expected server / Hyperconverged Management services can be further defined by the following high-level service requirements:

Service	Description
Installation and configuration services	Refers to the appropriate installation and configuration of the server environment as per industry best practice as well as OICL's policy requirements.
Monitoring operations	Provides processes and procedures to monitor the server environment to ensure that the appropriate monitoring, reporting and maintenance activities occur.

Operating system support	Provides for operating systems and related software configurations. The service also consists of ongoing processes to maintain supplier supported operating platforms for preventive software maintenance Services. This includes services such as: 1) Software configuration management 2) Software upgrades and patch management 3) Software release management 4) Software optimization, tuning and preventative maintenance
Hardware support	Provides the services and methodologies that will be used by the Bidder to support the OICL's server requirements. This service consists of the following components: 1) Hardware installation and configuration 2) Hardware environment support 3) Hardware preventative maintenance 4) Hardware refresh
Operating system security administration	Operating system security administration provides the processes to manage access to client assets at an operating system level. This security service provides the management of user logon ids and their access rights to system level resources, as well as maintaining server level security parameters and security product options. This section describes the various actions to be taken as part of the Security Administration Service, as well as what is needed on behalf of the client in order to provide these service levels.
System vulnerability management	Vulnerability management consists of preventive and detective services to identify vulnerabilities as they emerge; to prevent those vulnerabilities from affecting the in-scope systems; to detect when an in-scope system has been affected; and to cure those affected systems. Vulnerability management consists of both Vulnerability Alert management and Vulnerability Scanning processes. Vulnerability Alert management is the preventative process that collects known vulnerabilities and prioritizes vulnerabilities based on associated risk.
Operating system Security event logging	Operating system security event logging is a detective control that enables the recording of security events on system hosts based on present parameters. The administrative tool's logging function is enabled, and the security events are retained in a record for future review.
Performance and capacity management	Consist of the support processes to collect, monitor, and analyze system performance information, for processor usage, input/output (I/O) throughput activity, disk usage, and memory usage
scheduling and monitoring	Scheduling and monitoring Process consist of those specific tasks associated with administering the automated scheduling system to provide the tools and processes necessary to support a scheduling and monitoring processing environment.

Failover management	Provides for the recovery of the critical workload on the server environments in the event of an outage of primary server and / or a disaster. The bidder is required to prepare documentation of a written recovery plan for the server environments

1. The scope of work mentioned is illustrative and not exhaustive. The bidder needs to comply with OICL's requirements and any statutory or regulatory guidelines
2. Shifting of servers within the premises and reinstallation and configurations including cabling and asset labelling
3. Provide server configuration reports and configuration details to the OICL as requested
4. Maintain accurate supplier contact information and escalate to supplier contacts in a timely manner.
5. Implement configuration management processes and procedures.
6. Record and plan release of server upgrades and support its implementation.
7. Maintain an audit trail of server configuration changes as resulting from release and change control processes.
8. The required software agents are to be installed, configured and monitored.
9. Provide guidance to the OICL and industry best practice for the optimal configuration of the operating system environment.
10. Produce and maintain installation and configuration diagrams of all installations
11. Actively manage and report on the availability of all servers.
12. Perform server periodic checks, monitoring and performance tuning.
13. Communicate any service issues or implementation concerns with the OICL and appropriate support personnel and/or vendors.
14. Monitor hardware and system software status, process status, and take necessary action based on detected problems or issues as provided in this schedule.
15. Provide problem escalation and interact as necessary with third party suppliers.
16. Provide monitoring and troubleshooting for the server environment
17. Provide timely notification and escalation to on site personnel if any hardware and software conditions exist that must be resolved on site to meet the service levels provided in this schedule.
18. Bidders will ensure appropriate resources are on site to ensure service levels are achieved if recovery or corrective actions are required.
19. Propose tools for operations such as monitoring, deployment and configuration etc.
20. Ensure server access is secure and authorized.
21. Management of logical access to the server environment in accordance with the OICL's policy (including administrator \ root access)
22. Assist the OICL with application support requiring operating system changes or access
23. Evaluate the impact of new operating system upgrades or releases on existing applications and performance.
24. Install patches as and when these become available, per vendor instructions for security exposures and Operating System bug fixes deemed critical by the vendor.
25. Ensure the configuration of operating systems is in line with standards and policies as defined by the OICL
26. Document and track all configuration management problems using the site change management process.

27. Co-ordinate all changes through the site's change management process.
28. Configuration management for operating system release levels, patches and status.
29. Perform routine system operation functions and system console operations actions such as power on/off, system reboots, and start/stop/reset.
30. Apply preventive and corrective maintenance to all system level software (operating system and other non- application software).
31. Install and upgrade all system level software (the operating system and other non-application software).
32. Escalate hardware related malfunctions to the hardware supplier for resolution as provided in the vendor maintenance contract
33. Inventory information about hardware shipping and receiving, raised floor space requirements, equipment placement, cabling, fibre, connectivity details, power and earthing requirements
34. Servers/Storage hardware maintenance and support is based on various maintenance levels.
35. Alert the OICL about hardware changes that may impact application execution in support of the OICL's application testing.
36. Design back-out processes to return to the former hardware configuration if unforeseen problems occur during installation.
37. Co-ordinate the scheduling and installation of supplier- recommended preventative maintenance and other hardware specific changes.
38. Schedule down time as and when required to perform required hardware preventative maintenance, installation and testing.
39. Design, build, schedule, and implement a hardware refresh template.
40. Configure operating systems at the setup of each server, to establish super user privileges and access rules and establishing other standard guidelines, based on the agreed security policy of the OICL
41. Establish the process and procedures for requesting logon IDs and OS system level access
42. Create, modify, and delete system logon IDs using the Change Control Procedure
43. Monitor and maintain accounts and IDs and their designated privileges or access to make certain only active, authorized IDs have access, based on the agreed security policy.
44. Remove inactive or suspended IDs after a specified amount of time, based on consultation with security administration and the OICL's using the Change Control Procedure
45. Adjust and maintain operating system and security software parameters for password expiration, available in the specific operating system environment to meet the agreed security policy requirements
46. Provide processes and procedures to maintain operating system data protection options.
47. Perform bi-annual re-verification of data owners, authorized submitters and logon IDs, existing level of privileges, based on input from the OICL and system security configuration.
48. Work with the OICL's application support personnel as reasonably required for the Quarterly reviews and maintenance of inactive user id's
    - Compile a list of defined users id's on the Operating System, and provide list to the OICL
    - Perform reviews of system, monitoring and database administration user id definitions.
    - Bidders will apply the necessary changes as per the outcome of the review.
49. Hardening of servers as per OICL's policy
50. Anti-virus scan and anti-virus update on the server

51. Bidders will delete the OICL's application user id definitions, once such a request has been forwarded by the OICL.
52. Bidder to update virus related signature files on servers to manage the removal of malicious code.
53. Support and ensure that the timely installation of updated signature files and anti-virus software patches on all servers within the managed environment occurs.
54. Coordinate with OICL's SOC Vendor for receiving the most up-to-date information on malicious code outbreaks and the appropriate software signature files to protect against malicious code.
55. Obtain and release signature files for testing and application into a client dedicated environment.
56. Signature file and patch updates to be made available and installed utilizing the OICL's change control process.
57. Testing of signature files are to be performed prior to deployment.
58. Perform pre-production scans to identify potential security risks on a server prior to entering the production environment.
59. Review the results of vulnerability scans and determine corrective actions based on the results of the scans
60. Review the results of penetration testing and determine corrective actions based on the results of the scans.
61. Review government and supplier bulletins and various other sources to identify emerging threats or vulnerabilities to the OICL's hosts.
62. Maintain the risk evaluation process of vulnerabilities in which mitigation plans are determined, in accordance with the agreed security policy.
63. Maintain a vulnerability correction process to correct vulnerabilities detected through scanning of servers.
64. Maintain a vulnerability correction process as new vulnerabilities are identified.
65. Correct known vulnerabilities detected within the scope of the Bidder's responsibility, using the appropriate correction and change management processes.
66. The agreed security policy is to form the basis of security level.
67. Maintain processes to provide consistent configuration of parameters for logging devices and ongoing maintenance of those parameters.
68. Make certain of adequate retention of security event logs, based on the agreed security policy.
69. Configure the parameters of the administrative tools for all system hosts, in accordance with the agreed security policy.
70. Will provide event logging to the extent that tools, resources, and storage are available on client owned environments
71. Ensure sufficient storage capacity available to retain logs
72. Provide a listing of resource access rules for re-verification purposes
73. Perform quarterly review all user ID's and forward list of ID's not used for the last 6 months to the OICL for permission to delete these ID's.
74. Process security data identifying logged or audited access to a resource.
75. Process security data identifying attempted access to a protected resource.
76. Process security data identifying password violation attempts.
77. Process security data identifying usage of emergency ID's.
78. Monitor and maintain ID's and their designated privileges or access to make certain that only active, authorized ID's have access.
79. Adjust and maintain operating system and security software parameters, consisting of password expiration, available in the specific operating system.

80. Provide performance management functions and establish performance monitoring thresholds for major processes.
81. Proactively identify performance problems and improvements.
82. Provide capacity planning processes, for short term and long-term planning, forecasting resource requirements, and analyzing and reporting resource trends.
83. Monitor server utilization, CPU usage and I/O activity, produce capacity projection reports and develop plans for improvements.
84. Review server capacity and advice where future additional capacity may be required or archiving policies need reviewing or implementing.
85. Use standard operating system utilities and/or other third-party tools where appropriate, to project the effects of new changes and workload changes or when large configuration changes are performed in the environment on request of the OICL.
86. Perform operating system software tuning \ optimization as required to maintain day-to-day operations
87. Provide, install and maintain performance monitoring software.
88. Maintain system parameters to manage subsystem performance and workload throughput.
89. Implement changes as necessary to optimize the effectiveness and efficiency of the server platform.
90. Analyze system resource and storage utilization.
91. Perform capacity trend analysis.
92. Perform capacity modelling.
93. Capture capacity usage for the last 12 months.
94. Provide forecasting based on historic trends and planned OICL's initiatives.
95. Provide assistance with batch scheduling issues and problems using the problem management process.
96. Process job dependency information for batch job cycles as defined by the application support staff.
97. Maintain specific batch cycles utilizing the standard operating system CRON scheduler throughout the operational support coverage hours as necessary to meet defined service levels.
98. Provide appropriate system resources, tools and procedures to support the processing of user-initiated batch jobs.
99. Agree with the OICL prioritization for scheduled, ad hoc and system jobs.
100. Provide the necessary operational resources to support OICL-submitted or OICL-scheduled batch processing.
101. Maintain tools and facilities for OICL to perform batch scheduling and batch monitoring activities.
102. Log problem records if scheduled and automated batch jobs fail.
103. Consult with the OICL should job priorities require a change due to system constraints.
104. Perform problem diagnosis and purging of jobs on Operating System as necessary.
105. Monitor automation tools and functionality.
106. Maintain and execute system start- up/shutdown processes.
107. Monitor, identify, and implement automation techniques to remove manual interventions for ongoing monitoring and operation activities.
108. Perform maintenance and support for automation tools and products
109. Problem determination and isolation for automated operational processes.
110. Maintain and update documented hardware, facility, operating system, database and related system software recovery plans as necessary.

111. Perform quarterly tests of the recovery plans to verify the effectiveness there-off in supporting the day-to-day OICL operations.
112. Provide the required personnel resources to perform recovery plan drills or actual recovery plan execution at the time of disaster.
113. Provide requisite mirroring and redundancy across the DC & DR facilities to ensure adequate failover for the server environments.
114. Cluster configuration including the integration of startup/shutdown scripts
115. Configuration of shared storage
116. Provision of documentation on implemented high availability solution
117. Installation, maintenance and monitoring of clustering
118. Conduct Cluster tests as a part of DR drills

2.6.2.1.3 Storage Management

Storage and data consist of a system managed storage strategy that enables all data to be managed individually and automatically by the system. Within the system managed storage environment are both online and removable storage media, commonly referred to as disks and tapes. OICL requirements for data availability, accessibility, performance, and retention can be accommodated at the data set level and used by the system managed storage environment to select the correct media.

The expected storage and data management services can be further defined by the following high-level service requirements:

Service	Description
Mirroring	Includes the management of the SAN environment to ensure the availability, integrity and redundancy of OICL's storage environment across DC, DR and Near Site
Configuration	Process of organizing and maintaining storage information to streamline the process of maintenance, repair, expansion and upgrading.
End to end storage monitoring	Continuous monitoring of a DC & DR Storage Equipment notification to the administrator(s) in cases of failure / outages.
Archiving	implementing and maintain OICL's archive strategy as part of ensuring effective usage of storage resources.
Media management	Management of the associated media and peripheral equipment used for data storage (e.g. tape management)

1. The scope of work mentioned is illustrative and not exhaustive. The bidder needs to comply with OICL's requirements and any statutory or regulatory guidelines
2. Develop and document storage and data management requirements and policies.
3. Develop and document procedures for performing storage management that meet requirements and conform to defined policies
4. Review Storage Management procedures on a regular basis to be defined.
5. Provide appropriate data storage services (e.g. RAID array, SAN, tape, etc.) compliant with the agreed service levels and performance and availability metrics
6. Monitor and control storage performance according to data management policies.
7. Maintain and improve storage resource efficiency and space requirements.
8. Perform data backups and restores per established procedures and service level requirements as well as in accordance to the OICL's change management process.
9. Adjust the backup and restoration plan as new components are added to the system or availability requirements change
10. Provide input processing, for activities such as loading and rotation of third-party media (e.g. tape) and receipt and/or transmission of batch files, or large files.
11. Define storage management reporting requirements
12. Provide storage management reporting as defined by the OICL
13. Maintain the integrity of storage media, e.g. tape and disk.
14. Maintain the data integrity across DC & DR
15. Perform the relevant maintenance activities to ensure data availability and redundancy
16. Management of all third parties required to support the storage and data environment
17. Storage Management administration – manage and (Pro-active) monitor to ensure all time storage availability.
18. Resolve incident/problem related to storage as per agreed SLA.
19. Supporting new and existing storage products and services like replication, mirroring, security, traffic analysis, compression, virtualization etc.
20. Managing of physical storage elements/equipment
21. Managing moving inactive data off of production machines to free online disk space for important active data
22. Managing logical storage elements like caching, I/O technologies, data protection technologies etc.
23. Storage provisioning. Estimate and recommend storage requirements
24. Performing data management including backup and recovery
25. For disk storage, responding to storage requests by:
    - Allocating raw storage
    - Defining logical volumes
26. Troubleshooting disruptions and working with vendors to resolve the issues including software/firmware/patches related issues
27. Performing capacity management of storage resources to meet business needs
28. Planning for upgrades to hardware and software (including execution)
29. Granting OICL access to the storage management system from all applicable locations where the Services are performed, and allowing OICL to monitor and view the knowledge database on an ongoing basis (including Authorized Users)
30. Storage provisioning, purging of disk space, Replication support, LUN, SAN Switches, FC Links, Point in time copy / Snapshot management, RAID Configuration

31. Supporting Disaster Recovery activities pertaining to storage devices
32. Enable Proactive monitoring to ensure Minimal/Zero system disruptions/performance issues/outages.
33. Incorporate takeaways from Major Incidents into monitoring to prevent repetitions.
34. Maintaining documentation of configurations (including pictorial representation of the storage layout.)
35. Maintaining documentation of storage component details including architecture diagram, policies and configurations and the same should be reflected in the Configuration Management Database (CMDB)
36. Performing any other day-to-day administration and support activities

2.6.2.1.4 Backup and Restoration Management services

The scope of work mentioned is illustrative and not exhaustive. The bidder needs to comply with OICL's requirements and any statutory or regulatory guidelines The Bidder shall define data backup and recovery requirements. These requirements should cover the following at a minimum:

1. Identify the data backup technique which best suits the needs of OICL for in scope application /database/ server
2. Install, configure, test and manage any tools that may be required for data backup and recovery, such as those for writing the same data to multiple storage devices at the same time
3. Restore data to the database, as appropriate while ensuring that there is no loss of information / data.
4. Development of procedures and templates. Periodically conducting restoration drills, recording the results and reporting the results to OICL.
5. Execute backup and recovery procedures
6. Restore required files and data sets
7. Performing mock system failure and then data restoration drills on periodic basis
8. Manage all existing and all future deployments of, Backup and Restore Infrastructure. Media will include both tape and disk drives
9. Performance tuning for the Backup and Restore Infrastructure
10. Install and configure new equipment as required
11. Configure any new Backup and Restore infrastructure to the Monitoring and Alerting system and commence the Monitoring activity upon completion of the installation.
12. Provide capacity planning on backup and restore platforms.
13. Equipment shifting within the premises including reinstallation/ configuration and calling & labelling

Administration

14. Backup and Restoration Administration - Manage and monitor backup and restoration activities.
15. Provide Backup and restore infrastructure configuration maintenance

16. Handling backup (Full, Differential, Incremental) of agreed data for all managed servers as per the frequency (daily, weekly, monthly, yearly) defined in the backup & restore policy/ procedure/ guideline of OICL.
17. Performing media management for offsite/onsite backup
18. Handling service requests on backup and restoration.
19. Generating daily/weekly/monthly report on the backup/restoration performance
20. Performing retrieval of backup data
21. Performing back up media maintenance:
    - Defining media rotation requirements and/ or follow standard procedure
    - Labelling backup media as per backup policy
    - Planning and requisitioning of storage media
    - Monitoring and maintenance of the scratch tape pool
    - Registering tapes into automated tape handling devices
    - Destruction of media coming out of service in accordance with back up policy
22. Executing database back-ups and restores (including export and/or import) using database tools.
23. Performing restoration activities:
    - Testing of the restore the Data as per OICL Policy/guidelines.
    - Restoring complete or incremental backup as authorized (including user approval for restoration to same path, business manager approval for restoration of common folders to same path and OICL IT approval for all other restorations) within 24 elapsed hours
    - Periodically verifying backup media integrity and testing of backup and restoration process as per a defined schedule
    - Restoring single or multiple objects from the backup media
24. Reviewing backup and restoration process and infrastructure, to reduce the backup or restoration windows
25. Monitoring the backup and report on backup logs. Reasons for backup failures are to be analyzed and reported.
26. Monitor tape hardware for malfunctions and monitor tape usage
27. Managing and maintaining of back up tape devices
28. Performing maintenance of appropriate documentation, in accordance with back up policy:
    - Maintaining a backup register
    - Labelling and tracking of tapes
    - Backup and verification Logs
    - Restoration Logs
29. Granting OICL access to the backup management system from all applicable locations where the Services are performed, and allowing OICL to monitor and view the knowledge database on an ongoing basis (including Authorized Users)
30. Rapidly resolving every backup request/incident/problem within mutually agreed timelines
31. Backup policies configuration, modification for file systems, databases on heterogeneous operating systems
32. Performing any other day-to-day administration and support activities
33. Perform periodic audits to ensure the proper cataloguing of media
34. Review compliance with physical specifications, retention periods and Security

35. Provide monthly reports of retired and disposed Tapes. The report is to also to account for the status of all the backup media in the storage, including new media added for the month.
36. Maintain the integrity of the tape library system
37. Monitor tape library for reliability and minimization of read/write errors during the entire retention period

Backup and Recovery - Restoration testing

38. Carry out mock restoration tests
39. Decide applications and data for testing through restoration testing as per OICL policy
40. Document test plans and results
41. Delete data from test servers
42. Review restoration test results
43. Storing backups and managing media life expectancy for storage media, etc.

Tape Vaulting Services

As part of the Offsite media Management the cloud provider needs to do the following

- Integrity Checking
- Compliance with OICL and/or government requirements
- Tape Media needs to be store in secure off-site vault storage of the cloud provider
- Prepare media for off-site storage and store the same
- Log all physical tape Media in and out of the Data Center and/or remote locations, as appropriate.
- Maintain the rotation of the tape Media that is required for off-site storage.
- Periodically Audit the off-site tape storage facility for compliance and control procedures and provide reports of such audits to OICL.
- Maintain the integrity of data shipped to off- site storage
- Notify OICL of any problems
- Design an emergency tape Media return process and submit to OICL for approval
- Comply with, and review compliance with, physical specifications, retention periods, and security
- Wipe/erase the data and configuration information resident on the External Storage Media using recognized industry standards prior to disposing of the External Storage Media.

Replication

44. Monitor the RTO and RPO of complete solution as per the OICL's policy
45. Monitor and manage the replication between the DC and the DR
46. Generate reports to review the performance of the replication
47. Ensuring the RTO and RPO are maintained of the Complete solution as per the OICL's policy

2.6.2.1.5 DC – DR Drills

The scope of work mentioned is illustrative and not exhaustive. The bidder needs to comply with OICL's requirements and any statutory or regulatory guidelines. After implementation of the supplied hardware and software bidder need to perform the first DC DR Drill in totality within one month in coordination will all other vendors of the OICL through ADR solution.

1. Bidder need to perform minimum of 4 DC DR drill in each year during the contract period as per the discretion of the OICL.
2. All the DR Drills needs to be done from the supplied ADR tool
3. Bidder needs to allocate adequate resources, do project management and work closely with the application owner for performing the DC-DR Drills whenever planned by the OICL.
4. Any configuration level changes which can impact the DC DR drill need to be informed to ADR team before handover to avoid issues during the Drill.
5. During DC DR drill bidder need to allocate appropriate resources onsite to avoid any failure and delays which will be penalized appropriately as mentioned in the Section 7 Service Level of RFP
6. Bidder need to perform project management and all reporting and pre and post environment preparation to avoid any failure in the drill.
7. Maintain and update Business Continuity plan
8. Maintain and update disaster recovery plan
9. Ensure successful replication between production and DR
10. Notifying OICL promptly if a Disaster recovery scenario/condition arises
11. Assisting OICL in execution of DR plan in such scenario
12. Perform periodic recovery testing
13. Developing and executing test plans as per defined periodicity or as and when required
14. Documentation for Business continuity plan, Business continuity strategy plan & Roles and responsibility matrix for DC and DR team
15. Coordinate with all the users involved in DR testing
16. Track and report DR test results.
17. Develop an action plan and timeline to address DR testing results.
18. Implement DR action plans and provide ongoing status reporting until completion of all action items.
19. Initiate the DR plan for OICL in the event of OICL declared DR situation as per OICL Disaster Recovery policies and procedures.
20. Perform quarterly DC-DR drills based on OICL's periodicity.
21. Coordinate with OICL and third parties during a DR situation as per OICL Disaster Recovery policies and procedures.
22. OICL can also do an unplanned DC-DR Drill which bidder needs to support and design the system accordingly.

2.6.2.1.6 RTO / RPO Management

The bidder needs to maintain the below RTO and RPO parameters of the all the in-scope equipment's and software as mentioned below. Bidder will be responsible to main

Application Name	RTO / RPO
Portal & Mobile app	RPO: - 30 Minutes RTO: - 60 minutes

2.6.3 Cross Functional Services

Over and above the defined scope of services within the Domain Services, it is expected that the Bidder provide the IT support service management activities required to effectively manage the services required in a consistent, efficient and reliable manner and is able to meet the desired service levels.

The Cross Functional Services are mentioned below:

Service	Description
Incident management and IT Infrastructure Support Services	Incident management refers to an unplanned interruption to an IT Service or a reduction in the Quality of Service. The objective of incident management is to restore normal operations as quickly as possible with the least possible impact on either the business or the user. The Bidder is expected to assume accountability for the resolution of incidents as part of the 1st line of support to be provided. All 2nd level support will be the Bidder's responsibility. The Bidder should also take into account that a 24x7x365 support service is required. Bidder will raise tickets with respective OEMs for level 3 support.
Change Management and Release Management	Change Management will protect the production environment and its services. All changes to Configuration Items must be carried out in a planned and authorized manner. This includes identifying the specific Configuration Items and IT Services affected by the Change, deploying the Change, testing the Change on UAT environment, and having a roll back plan should the Change result in an unexpected state of the Service. Release Management will take a holistic view of a Change to an IT service and to verify that all aspects of a Release, both technical and non- technical
Service Level Management	Service Level Management will maintain and gradually improve business-aligned IT service quality through a constant cycle of agreeing, monitoring, reporting, and reviewing IT service achievements and through instigating actions to eradicate unacceptable levels of service

Security Management	Security Management will ensure compliance to security policies, contractual requirements, regulatory/statutory requirements, and as expressed in the Service Levels
Patch Management	Provide patches management services for in-scope infrastructure at DC & DR
Software License Management	Manage compliance with all Software licenses by monitoring and auditing all Software use, regardless of financial responsibility for the Software.
IT service continuity and Disaster Recovery	Supporting disaster recovery activities in scenario of a disaster and to keep the OICL disaster recovery plan up to date

2.6.3.1 Incident Management and IT Infrastructure Support Services

The Bidder should not only take precautions necessary to minimize damage from incidents and malfunctions, but also monitor and document these incidents in detail with a view to learn from them. The bidder should design and implement formal systems and procedures for detecting and reporting incidents relating to exceptional situations in day-to-day administration of the IT infrastructure. It should ensure that incidents are reported in time to enable authorities to take appropriate corrective actions to avoid the recurrence of such events in future.

Incident Management and IT Infrastructure Support Services

1. The scope of work mentioned is illustrative and not exhaustive. The bidder needs to comply with OICL's requirements and any statutory or regulatory guidelines
2. Receiving incidents through helpdesk tools and taking necessary action. The successful bidder shall update the status of the ticket as and when desired
3. The bidder will have to ensure that categorization of services is possible/enabled in the system to capture the defined SLAs
4. Providing updates to OICL's Team on incidents logged
5. Receiving requests and trouble reports, assign priority based on agreed upon definitions and route the request to the appropriate service engineer (including for remote support or on call support) and track till resolution
6. Resolving all incidents as per resolution time limit specified
7. The resolution time will be measured from the time when Bidder receives an intimation (through helpdesk tool /phone /email) from the group/end user. Resolution of problem for the purposes of this Service Level shall mean to achieve normal operational functionality
8. Define help desk call prioritization guidelines, problem severity codes, and escalation procedures
9. Provide L1 & L2 support for infrastructure calls
10. Level 1 Support for the Infrastructure & other queries linked with in-scope equipment & services
11. Conduct a thorough Root Cause Analysis to identify the problem and do an assessment requirement for routing it to L2 or AMC / ATS Support
12. Escalate and communicate issues as per agreed escalation/communication processes

13. Carrying out root cause analysis and corrective action for recurring incidents and for all critical and major problems.
14. Subject to OICL's review and approval, developing and periodically updating problem escalation procedures and distributing such procedures to Authorized Users
15. Escalate the tickets to Level 2 Support group for resolution.
16. Resolve the L2 problems logged by the users. Logs calls with AMC / ATS service providers in case of needs and coordinate and follow up with them till closure
17. Coordinate with Application / Hardware service providers to get the calls resolved which needs their support for ticket closure.
18. Support for the IT peripherals at DC & DR
19. Ensuring approval from OICL for moving out a helpdesk personnel
20. Notifying users of problem status and resolution through the Helpdesk system.
21. Monitor the resolution of the tickets
22. Manage problem escalation procedures
23. Providing status of pending requests to OICL business user -The mail should contain business, domain type, company code, person who raised the ticket, description of the incident/problem, actions taken, current status, last contacted personnel and reasons for pending status
24. Notifying OICL business users when request is completed
25. Resolution of the problems linked to in scope infrastructure or services
26. Notifying OICL IT of any deviation to process or failure to meet SLA
27. Developing the knowledge database that is required in order to solve as many incidents as possible as a first-time fix.
28. Knowledge database on an ongoing basis (including Authorized Users)
29. Liaison with the 3rd party Vendors, application service providers and coordinate problem identification and resolution
30. Record, analyze and report queries/tickets/calls received by the help desk, including:
    - Query volumes and duration,
    - Problem trends, and
    - Query resolution time.
    - Unresolved called
    - Age analysis of unresolved queries
    - Problem solution and resolutions
31. Conduct trend analysis and if required forward the case to the incident management team
32. Generate the reports from the system to track the Helpdesk support service levels
33. Dispatch the appropriate support personnel to remedy a problem if it is a hardware, network or security infrastructure related issue
34. Bidder will provide Induction Training to all the bidder personnel joining OICL account covering the following aspects:
    - Introduction to OICL's IT policies and processes
    - Understanding of OICL Business Processes and culture
    - Adequate training on new products and services
35. Performing any other day-to-day administration and support activities

2.6.3.2 Change Management and Release Management:

As part of the change management process the bidder is expected to perform the following activities:

Service Requirements	Description
Initial user request	In case of changes required to application software maintained by the bidder, the user shall submit the requirements to the OICL IT Team. The bidder must populate the 'Change Requirement' form. The requirements could relate to changes required in the operational infrastructure to support new/existing requirements or frequent error messages indicating that some parts of the programs are incorrect. The requirements could relate to additional features required to be
Approval of request	1. Once OICL provides the go ahead, the bidder along with the Bidder team, shall conduct a feasibility analysis 2. Subject to the outcome of the feasibility study, the request shall be forwarded to the relevant team. 3. An enterprise-wide, standard naming convention for each Hardware change requests must be adopted by the Bidder. This naming convention should clearly and unambiguously highlight the respective application / Hardware name, module name and the version number. 4. The Bidder, should collate the relevant information to assist OICL in analysing the Change Request based on the following: • Criticality and need for program change • Exploring new ways of getting the same functionality within the existing set up • Building workarounds • Effect on other modules/ menu options/ business process – Impact Analysis • Any possible effect on existing control procedures 5. The Bidder shall formally provide its recommendations to OICL.
Documenting the changes	The Bidder shall maintain the documentation related to the IT infrastructure and accordingly make the necessary modifications/updates as and when changes are made to programs. The Bidder must ensure that the user operating manual as well as system documentation is updated on a timely basis. The responsibility of maintaining the above documents is with the Bidder.

1. The scope of work mentioned is illustrative and not exhaustive. The bidder needs to comply with OICL's requirements and any statutory or regulatory guidelines

2. Apply change and release management policies, procedures and processes to comply with service level requirements
3. Establish change classifications (impact, priority, risk) and change authorization process.
4. Participate in the development of the change management and release management procedures and policies.
5. Document and classify proposed changes to OICL services. Documentation shall include OICL cost and risk impact if needed and back out plans for all proposed changes.
6. Develop and maintain a schedule of planned changes and provide to OICL as required, complying with change control process.
7. Determine change logistics and schedule.
8. Schedule and conduct change management meeting to include review of planned changes and results of changes made.
9. Attend weekly CAB meetings for approval of change implementation.
10. Attend change management meetings.
11. Provide change management documentation and tooling as required.
12. Review change management details and suggest amendments as appropriate to meet the needs of OICL (back out plan, go/no go decision).
13. Notify OICL of change timing and impact.
14. Implement change and adhere to detailed release plans.
15. Modify configuration, asset management items and service catalogue (if applicable) to reflect change. Asset management is reviewed quarterly but also can be requested on demand (referred later). Disaster recovery impact is covered under the normal change control processes.
16. Verify that completed changes delivered the expected impact and resolve negative impacts.
17. Monitor changes and report results of changes and impacts.
18. Conduct user acceptance tests as required.
19. The 2 resources which will be deployed by the bidder for doing the customization and development as per the requirement of the OICL will be dedicated for this activities and will not be part of any support / sustenance work.
20. As part of the process as and when a requirement is submitted by OICL for any customization / development these resources will be doing the feasibility study and provide the efforts (in Man-days) to OICL. Once get approval from OICL SRS and other development work will start.
21. These resources need to completed the work as per the efforts approve by OICL other wise In case of not adhering to the same a penalty of 1% (per shift cost of both resources) per week will be levied on the bidder.
22. In case if there are multiple demand as the same time then OICL will be using the extra Man days effort as asked in the RFP and the process and penalty of the same is as below

    - As part of Change Management bidder needs to note that during Sustenance period any change which OICL wants in any of the in-scope applications which will be under or equal to 25 days of Man efforts will be done by bidder without any charge. Any change will be above 25 days of Man efforts will be on CR Basis and the Man days rate will be applicable are the one provided in Bill of material at the time of submission.
    - For ex if any change requires a man days effort of 20 then it will be done by bidder free of cost however if any change require man day effort of 40 days, then OICL will pay for extra 15 days as per the rate quoted in the Bill of material.

- To make the change request timelines adequately in place bidder needs to know that during sustenance period for any change request timelines needs to be follow by the bidder. In case of not adhering to the same a penalty of 1% (Change request Value) per week will be levied on the bidder.
  - Bidder needs to factor minimum 2 resources for the Small CR which are between 5 to 40 Man Days of efforts
  - Bidder needs to factor minimum 3 Resources for the Medium CR which are between 41 to 100 Man Days Efforts
  - Bidder needs to factor minimum 4 Resources for High value CR which are between 100 to 200 Man Days efforts
  - Bidder needs to factor minimum 5 Resources for High value CR which are more than 200 Man Days efforts

According to the above matrix any CR which close for 40 Man days of efforts needs to go-Live within 20 days from the date of PO. CR Close for 100 Man days needs to Go-Live in 34 days and so on.

2.6.3.3 Service Level Management

The objective of the Service Level Management process is to manage and maintain the quality of IT services delivered to OICL's end users. The process should also seek to improve the quality of service delivered to the end users by reviewing the level of performance achieved by the IT Help Desk.

The Bidder is expected to design and implement a Service Level Management process to enable both the end user and the Vendors to have a clear understanding of the expected level of delivered services by documenting these goals in formal documents.

The SI is expected to perform the following activities in relation to Service Level Management with other IT processes:

1. Incident Management service assists Service Level Management by:
   - Monitoring and reporting on threshold breaches in agreements and notifying support officers when escalation and breach events occur
   - Providing information on historical data and trends
   - Providing the interface with customers on the level of services provided
   - Recording escalation actions and activities to maintain the service commitment under an SLA with the customer.
2. Problem Management service - assists Service Level Management by:
   - Identifying the underlying cause of incidents and problems to minimize their recurrence
   - Providing statistics, trends and historical data and assisting with Service Level Management reporting.
3. Change Management service assists Service Level Management by:
   - Providing information on the effect of changes on the IT infrastructure and the impact on service level targets before and after these changes are implemented
   - Tracking improvement in services since service levels are defined

4. Configuration Management service assists Service Level Management by:
    - Identifying the services affected by faulty configuration implementations
    - Identifying components/functions that combine to deliver a business function/service so that underlying agreements can be set up.
5. Assess and collate the Service Levels across multiple Vendor Contracts
6. Define, document, and implement a process to ensure that service levels are tracked
7. Develop a process by which reports are produced showing the performance of a service against its SLA
8. Undertake routine exercises whereby each SLA target is analyzed
9. Define, document, and implement a process that ensures that SLAs are regularly reviewed to ensure that they meet the OICL's requirements
10. Track the SLA in conjunction with the change management process, define, document and implement a process whereby all changes to SLAs are agreed upon and raised through the change management process using a request for change.
11. Provide periodic status on the Service Levels maintained across all the components/services that are required to be tracked
12. Compute the penalties based on the Service Level defaults
13. Collate the required documentation, evidence required to be shared with the respective Vendors

2.6.3.4 Security Management:

The Bidder must ensure that the ongoing operations adheres to OICL's security policy. The Bidder is expected to monitor and report any deviation from OICL's policies for the complete operations solution.

OICL's policies are in line with global standards like ISO 27001. Audits will be conducted by OICL (or by auditors and / or Consultants empanelled by OICL for the purpose.) Any findings unearthed during these audits will have to be fixed by the bidder. The bidder is required to ensure anti-virus scans and updates for the in-scope infrastructure.

The Bidder shall define a standard operating environment for OICL's IT infrastructure based on OICL's security policies. It shall also ensure that the required updates are performed as necessary.

The scope of work mentioned is illustrative and not exhaustive. The bidder needs to comply with OICL's requirements and any statutory or regulatory guidelines

1. Entire in scope IT infrastructure of the OICL complies with the Security Policy
2. Activities that would be carried out:
3. user ID creation / deletion,
4. password setting / resetting,
5. creation of limited access shared space on servers,
6. secured installation of assets, secured backup tape storage,
7. destruction of data on failed hardware components (for example, data on a server hard drive that fails) and
8. Confidential data protection methodologies.
9. Secure network resources against unauthorized access from internal or external sources.

10. Periodically review access authorizations and remove those for which approval no longer exists
11. Reset logon ID passwords and disclose passwords only to authorized personnel
12. Establish, change, deactivate, and remove logon IDs and associated access authorizations
13. Provide and maintain virus avoidance, detection, and elimination software for Servers.
14. Conduct periodic virus scans for Servers to monitor for virus propagation and perform virus detection and eradication
15. Maintain security controls for dial-in services and add users to the services as requested
16. Restrict physical access to Servers and infrastructure devices and other secured areas to authorized personnel only at DC
17. Restrict physical access to Servers and infrastructure devices and other secured areas to authorized personnel only at DRS
18. Implement controls which protect printed output and portable storage media (for example, tapes and disk packs) from unauthorized access and
19. Anti-virus update on the in-scope infrastructure
20. Anti-virus scan on the in scope infra

Security Incident Reporting

21. Report any significant computer security incidents occurring on any systems
22. Report any significant network security incidents occurring on any systems
23. Track the number of security incident occurrences resulting in a user's loss of data integrity, denial of service, loss of confidentiality or that renders the user(s) unproductive for a period.
24. Facilitate meetings with the OICL team
25. The Cloud Security would consist of the following layers:
    - Cloud Security Governance
    - Cloud Security Operations
    - Core Cloud Security Capabilities
    - Privacy
26. **Cloud Security Governance :-**
    MSP/ CSP should be capable of applying specific policies, principles, standards and guidelines to secure data and application deployed in the cloud. These policies and standards are to be applied with existing IT governance policies of the Govt. / OICL and not to be introduced in isolation.

27. **Cloud Security Operations :-**
    Cloud Security Operations to be able to meet the five-step process (Prepare, Prevent, Detect, Respond and Recover) under which various categorizes exist. Intrusion Detection & Prevention, Risk Assessment & Audits, Vulnerability Scanning and Remediation, Patch Management, Incident Response and Management, Investigation and Forensics.

28. **Core Cloud Security Capabilities :-**
    Identity & Access Management
    (Multifactor Authentication, Directory Services, Role Base Access Control , Single-sign-on (SSO) by adapting Identity-as-a-Service (IDaaS) for implementation of single sign-on) , CSP to restrict the use of root and generic accounts for Cloud Management and operations , CSP to

restrict the use of root and generic accounts for Cloud Management and operations , Zero trust IT security model coined by a Forrester Research Inc. that requires stringent verification of identity for each device and person trying to access resources on a private network, regardless of their position within or outside of the network perimeter to be implemented

29. Infrastructure Protection

One of the most critical aspect of any cloud deployment is protecting the underlying infrastructure (compute, network, storage) from any security threats. MSP/CSP to have state of art Security Operations Centre (SOC) facilities for monitoring and managing their deployed infrastructure.

30. Privacy

MSP/CSP to ensure Encryption of data in rest and in motion, Key Management to manage, create and protect encryption key and manage encryption and decryption tasks, Data Integrity and Data Handling are addressed to meet any regulatory or Departmental compliances.

31. Virtual Private Cloud for logical separation of infrastructure (server, storage, network) from other offerings of the Cloud Service Provider with strong/robust tenant isolation to be ensured

32. Data security in cloud

Encryption is key to protect and secure data in transit and data at rest. The following best practice to be adhered by the vendor/SI/MSP/CSP

o Multiple type of encryption to be implemented by CSP (i.e. Full Disk Encryption (FDE), Format Preserving Encryption, (FPE) Application layer Encryption, File Encryption, Database Encryption, etc.)

o For protecting data in transit, choose encryption of sensitive data prior to moving to cloud and/or use encrypted connections (HTTPS, SSL, TLS, FTPS, etc.) to protect the contents of data in transit.

o For protecting data at rest, Departments can simply encrypt sensitive data prior to storing them.

managed encryption options through HSM/KMS. Encryption key management to maintain controls of all private / public encryption keys

extra layer of data security via implementation of Data classification (Restricted, Confidential, Sensitive and Unclassified).

Ensure integrity of data while replicating from one site to another.

Backup (Full, Incremental, Differential) data regularly to ensure availability of data and perform periodic recovery operations to check correctness.

Ensure data-level monitoring is in place, and logs meet all the compliance requirements, if any, of the department.

33. Web application security

MSP/CSP/SI/Vendor to ensure Web application security by protecting web apps and services available over internet and accessed through a browser by implementing web application firewall to protect web applications by monitoring and filtering HTTP traffic between a web

application and the Internet. To protect the web applications from attacks such as, cross-site-scripting, SQL injection, file inclusion, as cross-site forgery, weak authentication and session management etc. Segregation: Web facing application should be deployed in DMZ (Demilitarized) zone and the Database Server should be deployed in the secured zone while deploying the application on cloud. Build security while initial design process of application. Application integration and information exchange to happen over secured API channels.

Security controls for interfaces and API's

Log and monitor API calls.

Use software-defined security to automate security controls.

Use event-driven security such Anti-virus, when available, to automate detection and remediation of security issues. Adopting security while designing the application through the process of DevSecOps is to be ensured for application security in the cloud.

34. Cloud Security Design Principles / considerations

The vendor /System Integrator/ MSP/CSP to ensure the following the key design principles for Cloud technology adoption:

1. Security at all layers: Ensure robust Security is applied to all layers (Physical, network, Data, Application, etc.) of their architecture with multiple security controls. This will ensure end to end protecting of application/data hosted by departments on Cloud platform.

2. Safeguard data while at rest and in transit: Identify and Classify the data in terms of criticality/sensitivity and define their levels. This can be prevented via using the available security controls like access control, tokenization, encryption, etc.

3. Monitoring and Auditing: Ensure monitoring, auditing and alerting is configured to capture the changes in the department's system in real time. Further, log integration and metric collection can automatically investigate, act and respond.

4. Access management and Controls: Ensure implementation of principle of selective privileges and impose segregation of duties with appropriate access and authorization. Centralized identity and access management can eliminate any unauthorized access and information loss/theft.

5. Readiness for security events: Department/CSP needs to prepare system for any unusual security event. Regular vulnerability and security tests need to be conducted to identify the security gaps and issues. Several drill can be conducted to record the response of the Cloud systems at different layers.

6. Automate security best practices: Automating software/hardware/Application based security system via AI/ML/Bots to improve the ability to secure environment which can perform regular checks and implement the controls needed to restrict the attack and enhance cloud security.

7. Cloud Vendor Lock-in: Departments to ensure that there is no vendor lock-in by Cloud services provider while hosting the application/data, as there is no standard guidelines between different cloud providers for data migration and exports, so it becomes difficult to migrate data from one cloud provider to another or migration to on-premise Data centre.

35. Standards applicable for Security

ISO 27001 and ISO 27002 for Information Security Management System (ISMS) compliance , ISO 27017 , ISO 27018 , Payment Card Industry Data Security Standard (PCI DSS) , SSAE 16/

SOC 2. MSP/SI/Vendor/CSPs to ensure and adhere to the latest regulatory compliances and certifications, along with having the certification renewed periodically.

36. Perimeter and Physical Security

Ensuring perimeter security and physical security of the Data Centre, shall be the responsibility of the CSP, and in accordance with the norms laid down for empanelment for Cloud Service Providers by MeitY. Unauthorized personnel gaining access to the data centre shall result in a compromise and the CSPs are responsible to ensure sufficient measures such as security guards, secured fencing, security scanners, biometric access, CCTV surveillance, Access Logs etc. are available at the data centre to prevent unauthorized or forceful entry into Data Centre premises.

37. Network Security

CSP to implement strong security controls for internal and external network separation / communication. CSP to ensure appropriate network segmentation which separates networks of different sensitivity levels. Use Virtual Private Network (SSL or Site to Site) to access Cloud infrastructure and services. Use IP Whitelisting to allow connections from certain IPs and deny all others where applicable. Pre-certifying additional VLAN, firewall ports and load balancers. Separate virtual networks and cloud accounts. Restriction of traffic between workloads in the same virtual subnet using a firewall policy needs to be followed whenever possible. Dependency on virtual appliances that restrict elasticity or cause performance bottlenecks needs to be minimized. Implement policies and internal security controls to prevent traffic monitoring without approval or outside contractual agreements and consumer networks modifications. An automated response to attacks should be configured and additional information on the intrusion must be acquired. IP blocking, connection termination and signature analysis are some of the processes under such an automated response. Regularly monitor network traffic logs or implement a SIEM to get real-time security alerts generated by application and network devices. Prefer use of SDN capabilities for multiple virtual networks and multiple cloud accounts/segments to increase network isolation.

38. Host/ Compute security

For critical workloads ensure High Availability at all deployment levels – compute, firewall, Load balancers.

To ensure that as soon as the new application server is deployed, security scans should be enabled, and the servers should be added to continuous monitoring.

Integrate security testing and policies while VM image creation.

Disable remote access post application configuration.

Implement appropriate role-based access controls and strong authentication for all Virtual Machines (VM), Containers and VM images.

Employ the use of pre-certified VM images from the cloud platform where precertification would be an on-going effort.

Prefer Patching of VM images rather than patching running instances. Ensure patching is up to date for Operating System, Database licenses etc.

Ensure VM level encryption through Bitlocker, LUKS etc. for security of VM in case of compromise

Ensure Operating System Hardening is performed on the virtual machine.

Take periodic VM snapshots and save in a secured repository.
Prefer use of file integrity monitoring in order to ensure authenticated changes and detect unapproved changes to files.
Store logs (including Audit logs) externally to workloads.
Install Anti-virus software on Virtual Machine and ensuring periodic patching is performed.
Perform periodic vulnerability assessments and penetration testing (VAPT) on Department's cloud infrastructure.

2.6.3.5 Patch Management

The Bidder will be responsible for implementing patch management for in-scope infrastructure at DC & DR

The Bidder shall perform system planning and design for patch management. Once this process is defined, Bidder shall configure the patch management set-up and test the patch management process. The Bidder shall develop the strategy for activation, including:

1. Which hardware must be activated first
2. Start times (e.g., nights and weekends when there is less line activity and less impact on performance)
3. Assignment of attended and unattended nodes
4. Identification of hardware which do not get updated and developing a plan to update the same.
5. Distribution of patches, services packs, reports etc.

Bidder shall take corrective action, as appropriate, for problems resulting from patch management (additions or upgrades) to facilitate application stability. Bidder shall monitor the asset management and software license management systems implemented at OICL.

Patch Management for end user computer/laptops, branch network equipment and branch peripherals are out of scope for the bidder.

1. The scope of work mentioned is illustrative and not exhaustive. The bidder needs to comply with OICL's requirements and any statutory or regulatory guidelines
2. Define patch management processes and procedures, packaging (Server software build), configuration customization, and deployment of patches
3. Perform system planning and design for patch management e.g. boot disks, tapes, server-based software)
4. Develop the strategy for activation, including:
5. Start times (e.g., nights and weekends when there is less line activity and less impact on End Users);
6. Assignment of attended and unattended Hardware; and Distribution
7. Check software configuration and ensure policy compliance
8. Document the patch management strategy for each application
9. Test all new releases of software prior to promotion into the production environment
10. Take corrective action, as appropriate, for problems resulting from software distribution (additions or upgrades) to correct error conditions and facilitate application stability.

11. Patch Management is only for in scope infrastructure at DC & DR. The end user devices are out of scope

2.6.3.6 Software License Management:

The Bidder shall perform an inventory of software licenses as of a date. The Bidder will develop and maintain a software license inventory data base which tracks:

1. Whether the license has been procured by the SI or by OICL
2. Whether the license comprises entitlement for software upgrades, enhancements, refreshes, replacements, and maintenance
3. The authorized end users who have access to the Server resources
4. Expiry of licenses and contracts.
5. Maintain software license inventory to include the licenses existing as of the Start Date
6. Maintain data regarding entitlement for software upgrades, enhancements, refreshes, replacements, and maintenance
7. Perform periodic audits to measure license compliance against the number of valid End User software licenses consistent with the terms and conditions of site license agreements, volume purchase agreements, and other mutually agreed upon licensed software terms and conditions
8. Periodically review of software license and maintenance agreements

2.6.3.7 IT service continuity and Disaster Recovery

The bidder is required to provide IT service continuity and disaster recovery services for OICL production environments and their associated infrastructure. The bidder must demonstrate that it will consistently meet or exceed OICL business continuity and disaster recovery requirements.

The scope of work mentioned is illustrative and not exhaustive. The bidder needs to comply with OICL's requirements and any statutory or regulatory guidelines

1. Maintain and update Business Continuity plan.
2. Maintain and update disaster recovery plan
3. Ensure successful replication between production and DR
4. Notifying OICL promptly if a Disaster recovery scenario/condition arises
5. Assisting OICL in execution of DR plan in such scenario
6. Perform periodic recovery testing
7. Developing and executing test plans as per defined periodicity or as and when required
8. Documentation for Business continuity plan, Business continuity strategy plan & Roles and responsibility matrix for DC and DR team
9. Coordinate involvement of users for DR testing
10. Track and report DR test results
11. Develop an action plan and timeline to address DR testing results
12. Implement DR action plans and provide ongoing status reporting until completion of all action items
13. Initiate the DR plan for OICL in the event of an OICL declared DR situation per OICL Disaster Recovery policies and procedures.
14. Perform quarterly DR drills or DR drills based on OICL's periodicity

15. Coordinate with OICL and third parties during a DR situation per OICL Disaster Recovery policies and procedures

2.6.3.8 Application Performance Management

Bidder needs to monitor the performance of Core Insurance Application and Portal its associated database on Daily basis in working hours of the OICL. The scope of the application performance management and assurance services should include, but not limited, to the following:

1. Preventive monitoring of Application (Core Insurance and Portal)
2. In the event of a critical Alert application experts would step in to carry out initial analysis and hand over the observations for the respective teams to action the same to prevent the event from happening.
3. Availability of senior level experts on On-Call Basis for critical alerts/incidents
4. Provide suggestive restoration/preventive advises as applicable to ensure stability of the environment
5. APM should minimize the application downtime and provide visibility on batch operations.
6. The APM and assurance services should provide the capability to have a deep dive analysis of infra (Web, App, DB, OS & Storage) component even post alert and reduce the MTTR on issues faced.
7. The proposed solution should provide support for in any other http, https or non-http applications and should have the ability to add environment specific custom KPI's.
8. Application Performance Monitoring and Management software should deliver L1 support from an independent third (3rd) party for the first year after implementation for24x7 Application Monitoring for Availability, Alert Management, Software Administration, Service Reporting and Incident Reporting and thereafter bidder can factor bidder resources for the management.
9. The L2 support should be provided by an independent third (3rd) party for the first year after implementation for analysis, remediation, software administration, reporting and incident analysis, troubleshooting and alert analysis and thereafter bidder can factor bidder resources for the management. The cost of the L1 & L2 resources should be factored in by the bidder in the Annexure 16 – Bill of material.
10. The Bidder is required to comply to Annexure 15- functional & technical specifications for APM tools.

2.6.3.9 Roles and Responsibility of APM, ADR, API gateway, Chatbot, password less authentication, HSM and KSM L1, L2 Resources

Bidder needs to provide the L1 and L2 onsite resources as per the Minimum number and Shift mentioned in the RFP. The scope of work mentioned is illustrative and not exhaustive. The bidder needs to comply with OICL's requirements and any statutory or regulatory guidelines

Role & Responsibility of L1 (Monitoring)

1. Monitor the Alerts triggered by Tools for various components / transactions across in-scope applications and hardware and intimate the respective stakeholders
2. Follow SoP's for various monitoring tasks as per discussions with application owners

3. Provide 1st level details to Application Owner around alerts during alerts' intimation
4. Maintain call logs for calls made to / received from application owners.
5. Continuously check Data Collection status of all components and transactions across in-scope applications and hardware
6. Raise tickets / tasks for administrator to work on data collection issue, if any.
7. Generate daily/weekly and monthly reports
    a) Data Collection Report - Critical/High/Low
    b) Transaction Volume Report
    c) Agent Health Report
    d) Application wise alerts
8. Coordinate with OICL's application team during any change-release events within the application.
9. Enable/disable Alert profiles as per request
10. Reset thresholds as per request from App Owner
11. Enable/Disable monitoring of components as per request from App Owner
12. Perform Tool health maintenance activities, such as DB Backup, services restart
13. Provide application specific Real Time Transaction performance details: Various parameters/KPIs include:
14. Volume of transactions (i.e., how many transactions have occurred in a minute)
15. Average response time of these transactions in a minute (Response time is the time from the instant a transaction hits a web server and returns a response out of the web server) are displayed.
16. Aggregated count of successful, failed and timed out transactions per minute are displayed.
17. Audit details like transaction start time, end time, client IP address and port, server IP address and port are displayed

Role & Responsibility of L2 (Analysis) and (Remediation)

18. Managing change request in tool given by Application owners such as agent reinstallation, adding custom components.
19. Managing Tool metadata & Sustaining Implemented applications
20. Tool System health check periodically (watching for errors in Tool, log file analysis)
21. Create and maintain Tool configuration & maintenance documentation.
22. Undertake advanced administration tasks as required e.g. to support problem resolution in tool
23. Responsible for tool Availability, Performance, analysis & remediation
24. Deploying patch updates as and when necessary, with Product Support team and OICL team
25. Understand information required & actions desired for various alert scenarios
26. Develops scripts for custom forensic actions/information
27. UAT testing of forensic scripts & approval onsite
28. Providing remedial measures: - Analyze the issue based on data issued-Narrow down to the layer in which the problem is predominant-For "High" severity alerts OEM to provide the suggestive restoration steps-prepare RCA document-Based on the Infrastructure component utilization trends proactive sizing recommendations
29. Provide Predictive Analytics

a) Component KPI alert generation based on transaction volume and component KPI correlation
b) any other as per OICL's requirements

30. Provide performance fine tuning for
    a) Slowdown of EOD BOD process
    b) Increase in response time
    c) Creation of deadlocks and causing Resource Busy Error
    d) Slowdown of Closing and Interest related batch jobs
    e) DB server utilization reaching up to 100%
    f) Queries from 3rd party application if any causing performance issues would be highlighted to OICL with any tuning recommendations (if applicable). OICL should take up with respective vendors or OICL's internal teams for fixing.
31. Interface with Tools OEM's support team for support requests and enhancements

2.6.3.10 Exit Management Services

In addition to the requirements mentioned in RFP, the purpose of this section is to provide details of bidder's assistance during termination or expiration of contract and exit plan strategy for the OICL. Bidder also has to develop a detailed Exit Plan with-in 6 months of signing of contract. After that, the exit plan has to be regularly reviewed and updated on a yearly basis.

Following shall be covered as part of the Handover & Transition of Services at the end of contract period or in the event of termination. The scope of work mentioned is illustrative and not exhaustive. The bidder needs to comply with OICL's requirements and any statutory or regulatory guidelines

1. If any other agency or service provider is selected by OICL for providing in-scope services, the Bidder selected through this RFP shall provide support for necessary handholding, transition, sharing of information and relevant documents and other related support to the complete transitions upto satisfaction of OICL. In case if OICL observes the lack of willingness to manage transit/ sharing of information or lack of support from bidder (selected through this RFP), OICL shall have absolute discretion to apply requisite penalties and deduct the amount from its billing or from performance guarantee.
2. Bidder shall provide the necessary transition for the period of 6 months. However, this period of transition could vary depending on the need of OICL and the same shall be communicated to them.
3. During transition phase, the Successful Bidder shall not change or remove their key resources at any locations to enable the successful transition. In case such instances, OICL will have right to penalize the Successful Bidder appropriately.
4. During transition phase, OICL will deploy a dedicated Transition Manager to enable the successful transition.
5. During the exit management process, it is the responsibility of bidder to address and rectify the problems identified with the IT infrastructure of OICL including installation/reinstallation of the system software, Databases etc. The Successful Bidder shall ensure that the infrastructure are handed over to OICL in an operational condition to the satisfaction of OICL.
6. The ownership of the assets (including soft and hard components existing and procured through this RFP) except for those which are taken as a service, at any point of time during

the term of the contract or expiry of the Contract, shall rest with OICL. In addition, any information/ data gathered or generated by the Successful Bidder during the term of the contract would be the property of OICL and the same should be handed over to OICL in native format at the end or termination of the contract.

7. In case OICL decides to withdraw any services/components from the Bidder's scope of work during the contract period, the Successful Bidder has to facilitate the transition of that service / components in compliance with above clauses.
8. Bidder shall provide the Termination/Expiration Assistance regardless of the reason for termination or expiration
9. Bidder shall fully and timely compliance with the Exit Plan
10. Bidder shall not make any changes to the Services under this Agreement and shall continue to provide all Services to comply with the Service Levels;
11. The bidder should perform a complete reverse transition of services to the OICL's selected new vendor.
12. Bidder shall within ninety (90) days of the Signing Date, deliver to OICL a plan specifying the Termination/Expiration Assistance including the functions and services of Bidder necessary to accomplish the transfer of the responsibility for the Services from Bidder to OICL or a Third Party, in the event of the expiry of the Term or the termination of this Agreement. The plan shall at the minimum, contain the Bidder's detailed plan for Operational and Knowledge Transfer requirements and list of documentation
13. The Exit Plan shall be updated by the Bidder on an annual basis in accordance with OICL's requirements and delivered to OICL for its approval on or before the start of each Contract Year.
14. Knowledge Transfer and Handover of Services
15. Bidder shall provide for a -transfer of knowledge regarding the Services
16. Provide to OICL personnel or designated third party personnel training in the performance of the Services that are to be transferred.
17. Bidder shall train personnel designated by OICL and/or its designee(s) in the use of any processes or associated Equipment, Materials, Systems or tools used in connection with the provision of the Services as needed for such personnel to assume responsibility for performance of the Services;
18. Provide to OICL and/or its designee(s) information regarding the Services as necessary to implement the Exit Plan, and providing such information regarding Services as reasonably necessary for OICL or its designee to assume responsibility for continued performance of Services in an orderly manner so as to minimize disruption in the operations
19. Provide OICL or its designee a complete copy of the OICL's IP in Bidder's possession or control and of the Bidder IP that OICL is licensed or otherwise authorized to use
20. Explain the change management process, problem management process, Policies and Procedures Manual, reports and other standards and procedures to OICL's or its designee's operations staff.
21. Provide technical documentation for Software used by Provider to provide the Services as needed for continuing performance of the Services.
22. Identify, record and provide release levels for Software and updating such records of release levels prior to and during transition of the Services
23. Provide assistance to OICL or its designee in notifying third-party vendors of procedures to be followed during the transition of Services

24. Ensure transfer of the Configuration Management Database (CMDB) that contains details of the data elements that are used in the provision and management of the Services. The CMDB must be in a form that can be migrated to a new environment that manages the Configuration Items
25. Bidder shall provide other technical and process assistance as requested by OICL and/or its designee(s).
26. The vendor will not be allowed to take any OICL's IP or information The Managed Service Provider shall not delete any data at the end of the agreement from the underlying CSP's Cloud environment (for a maximum of 45 days beyond the expiry of the Agreement) without the express approval of the Purchaser. The Purchaser shall pay to the Managed Service Provider the cost associated with retaining the data beyond 45 days. The associated cost shall be arrived at based on the cost figures indicated in the commercial quote submitted by the Managed Service Provider. (ii) The underlying CSP shall be responsible for providing the tools for import / export of VMs, associated content, data, etc., and the Managed Service Provider, in consultation with the Purchaser, shall be responsible for preparation of the Exit Management Plan and carrying out the exit management / transition related activities. (iii) The Managed Service Provider shall provide the Purchaser or its nominated agency with a recommended exit management plan ("Exit Management Plan") or transition plan indicating the nature and scope of the underlying CSP's transitioning services. The Exit Management Plan shall deal with the following aspects of the exit management in relation to the Agreement as a whole or the particular service of the Agreement: a. Transition of Managed Services b. Migration from the incumbent Cloud Service Provider's environment to the new environment (iv) The Managed Service Provider is responsible for both transition of the services as well as migration of the VMs, Data, Content and other assets to the new environment. (v) The Managed Service Provider shall carry out the migration of the VMs, data, content and any other assets to the new environment (alternate Cloud Service Provider or Data Centre) identified by the Purchaser to enable successful deployment and running of the Purchaser's solution in the new environment. Master Service Agreement - Procurement of Cloud Services Page 34 of 44 (vi) The format of the data transmitted from the current CSP to the new environment identified by the Department should leverage standard data formats (e.g., OVF, etc.) whenever possible to ease and enhance portability. The format shall be finalized in consultation with the Purchaser. (vii) The Managed Service Provider shall transition Purchaser's solution including retrieval of all data in the formats approved by the Purchaser. (viii) The Managed Service Provider shall ensure that all the documentation required by the Purchaser for smooth transition (in addition to the documentation provided by the underlying Cloud Service Provider) are kept up to date and all such documentation is handed over to the Purchaser during regular intervals as well as during the exit management process. (ix) The Managed Service Provider shall transfer the organizational structure developed during the term to support the delivery of the Exit Management Services. This will include: a. Documented and updated functional organization charts, operating level agreements with third-party contractors, phone trees, contact lists, and standard operating procedures. b. Physical and logical security processes and tools, including catalogues, badges, keys, documented ownership and access levels for all passwords, and instructions for use and operation of security controls. (x) The Managed Service Provider shall carry out following key activities, including but not limited to, as part of the knowledge transfer: a. Preparing documents to explain design and characteristics b. Carrying out joint operations of key

activities or services c. Briefing sessions on processes and documenting processes d. Sharing the logs, etc. e. Briefing sessions on the managed services, the way these are deployed on Cloud and integrated f. Briefing sessions on the offerings (IaaS/PaaS/SaaS) of the underlying Cloud Service Provider (xi) The Managed Service Provider shall transfer know-how relating to operation and maintenance of the solution, software, Cloud Services, etc.

2.6.4 Application Management

Bidder needs to provide the facility Management support to OICL after go-live of the Portal and Mobile app. The annual maintenance and support services would cover all the items as defined in section. It will be bidder's responsibility to locate the exact nature of the problem(s)/ fault(s) and rectify the same, if any, during the warranty and annual maintenance period.

OICL shall have one integrated help desk for all the initiatives being run by the corporation. This helpdesk shall be the Single Point of Contact (SPOC) for all business and IT services staff. This helpdesk will be the central collection point for service staff contact and control of the problem, change, and service management processes. This includes both incident management and service request management. The support (L1, L2, and L3) should be available from the day the new application goes Live at any of the OICL Offices or over the internet.

The Bidder has to provide the resolution / service as per the defined service levels. The Bidder has to make sure that the methodology proposed for addressing and resolving problems is aligned to the required and defined service levels.

The Bidder should staff persons in support who are conversant with the solutions deployed and are capable of resolving routine problems and queries through the service desk application or over the phone.

The minimum number of resources are provided in the RFP however bidder needs to size the number of resources to meet the SLA.

2.6.4.1 Level One (L1) Support

- Will serve as the front-end for all users (all the users internal as well as external) and provide services request sorting, information and non-functional information, ticket routing for support of the Application
- L1 would typically address queries all end user issues pertaining to:
- Business application related issues/queries,
- Operating System (Windows, Linux & Unix), Printing, Generic IT Queries
- Queries related to business process
- Other environmental software such as office automation tools etc.
- The key activities that the Bidder is expected to perform as part of Level 1 Support are:
- User Management
- Creation or modification of user profiles
- Assessment in case of specific rights assignment

- Provision for assigning user rights only for certain fixed period
- Categorization of requests into functional clarification, bug or change request
- Functional clarification / work around to be provided by Level 1 support itself
- L1 support team needs to do a recon activity every day where they need to generate the report for failed transaction and submit a report to OICL on the based of which OICL will be the issuance and processing of refunds for failed transactions.
- Bug change requests to be logged and reported for further processing
- Provide telephonic and / or electronic mechanisms for problem reporting requests as well as for service and status updates.
- Escalate/assign unresolved issues for L2 support

2.6.4.2 Level Two (L2) Support

OICL expects the Bidder to provide for L2 support for all in scope applications. The L2 support provided by the Bidder should be comprehensive and cover entire management and support of the Application developed and implemented by the Bidder. The expected indicative services are as below:-

- Provide continuous onsite support for the application being implemented
- Performing and troubleshooting End of Day, End of Month, End of Quarter and
- End of Year activity
- Resolve calls within stipulated timeframe as defined in Service Level Agreement
- Provide on-site trained personnel in each L2 shift, having adequate exposure and background on the solutions for problem handling and resolution
- Coordinate with the L3 teams for resolution and provide necessary information as may be required by the team to resolve the issues
- Escalate the unresolved calls as per escalation matrix
- Provide the timeframe for providing a solution of resolution of the escalated calls
- Prepare a root cause analysis document with the resolutions provided for major issues
- Problems which have resulted in complete service disruptions or downtime
- Critical production issues such as inconsistent accounting or system behaviour
- Delayed response times
- Data / table corruptions
- System Performance issues (high utilization levels)
- To decide on preventive maintenance schedule with OICL
- Liaise with the L1 support personnel for the call information and resolution
- Modifications to existing scripts, reports, due to errors / technical faults

- Present to the OICL management on the critical issues reported, resolved, solution provided and the suggested recommendations or leading practices as and when asked by OICL or on a monthly basis whichever is earlier.
- Provide recommendation on performance tuning of the application
- Perform the application audit on a half yearly basis
- Rectify any corruption in the software
- Ensure patch releases are ported to the production environment with no business disruption or business losses
- Perform application replication across the Data Centre and Disaster Recovery site to ensure zero data loss
- Provide application support from OICL"s data centre
- The Bidder is expected to act upon the tickets routed from Level 1. The Bidder must ensure proficient and professional personnel are put to handle the L2 support and resolutions are provided on a proactive basis
- L2 agents are expected to address issues/queries related to the business application. L2 agents will need to assess the cause of the issue and accordingly resolve the same within the timelines mentioned in the SLA. The agents would also need to track problems from initial call to restore to service
- All other activities as would be required by the Bidder to manage and maintain the solutions.
- Bidder needs to do a yearly code optimization exercise on logic written.

2.6.4.3 Level Three (L3) Support

Brief description of the envisaged activities to be performed by SI at L3 is enumerated as under. The services specified herein are not exhaustive and are only indicative.

- Resolve the call within the stipulated timeframe as defined under the service level agreements
- Communicate the status of the call to OICL and accordingly update the status, resolution or workaround and date of resolution in the appropriate tool
- Prepare a root cause analysis document for issues referred to L3 support and provide to OICL along with the resolution
- Liaise with the L2 support personnel for the call information and resolution
- Provide version upgrades
- All other activities as would be required by the Bidder to manage and maintain the application

2.6.4.4 Helpdesk Support

Helpdesk team will be the front-end team who will pick up all the call related to portal and mobile app from all stakeholders whether internal or external. Bidder needs to size the helpdesk support team appropriately. An indicative list of the helpdesk activities shall include the following minimum activities:

- Customer care call handling and email handling (this would include issue resolution on call)
- Daily reporting of calls received.
- Tracking of issues identified and monitoring them till their closure
- Co-ordination with OICL and system support team on issue reporting
- Generation of daily payment reconciliation report and providing it to concerned OICL official for approval/ further action.
- Managing the updation of master data in the portal (IDV updation, Office master updation, Employee Master updation)
- Monthly analysis of portal trends
- Daily MIS reporting to OICL
- Helpdesk requests for extending technical support on Portal functionalities
- Deployment of web-based tool for the helpdesk
- Provide Help Desk facility for agreed SLAs for reporting technical incidents / issues / problems with the system. Help desk facility shall be provided through a dedicated phone number
- Track each incident / call to resolution
- Escalate the calls, to the appropriate levels, if, necessary as per the escalation matrix agreed upon and developed by Bidder and OICL
- Analyse the incident / call statistics and provide monthly reports including but not limited to:
- Type of incidents / calls logged
- Incidents / calls resolved
- Incidents / calls open
- Update the frequently asked questions on Web Portal to assist end users in resolving basic issues themselves

2.6.5 Minimum Deployment of resources during Sustenance Phase

Bidder shall at minimum deploy the resources as per the minimum deployment level mentioned below during the Sustenance Phase

Bidder should independently arrive at the sizing and deployment plan to meet the RFP requirements (As per scope of work and SLAs) adhering the minimum deployment level during the Sustenance stage. Bidder shall deploy resources at no extra cost if the proposed deployment does not meet the RFP

requirements and SLAs. Bidder needs to mentioned that number of resources factored and the cost in the bill of material which OICL will pay during sustenance period. If during sustenance period if there is a need to deploy extra number of resources to maintain the scope and SLA then bidder will deploy at no extra cost to OICL.

Bidder needs to note that atleast 30% of the development resources (Portal and Mobile app) needs to retain by the bidder during full sustenance period so that there should be a proper knowledge of development and coding during sustenance.

Bidder also needs to factor 2 resources during sustenance period which will be dedicated for doing the customization and changes as part of change management and they will not be involved in any sustenance activities. Please refer to Change Management section for more details

Resource	Location	Minimum Number of Resources Per Shift	No of Shifts	Service Windows	Total Minimum Resources
L3- Techno Functional	OICL Corporate Office	1	1	10 AM to 6 PM	1
L1 – Portal & Mobile app	OICL Corporate Office	3	1	10 AM to 6 PM	3
L2 – Portal & Mobile app	OICL Corporate Office	3	1	10 AM to 6 PM	3
Change Management resources	OICL Corporate Office	2	1	10 AM to 6 PM	2

OICL reserves the right to demand the services of higher qualified professional on need basis for any escalated incidents if L2 Engineer is unable to resolve an incident in the agreed timeline. Bidder to provide the services of higher qualified professional accordingly with no additional cost to OICL.

2.6.6 Desired Qualification and Experience of Resources

Area	Role/ Description	Experience	Educational Qualifications/ Certifications/ Skills
Techno Functional	Program Manager/Service Delivery Manager	>10 years	• MBA/Engineering with PMI certification. ISO 20000 implementation certification will be an added advantage. • Should have experience of

			managing IT Infrastructure managed services (Servers, storage, database, networks, backup & restore, Quality Assurance and Helpdesk Management) and Business Application (Mobile, Internet) engagements in at least one BFSI in India
Application (Portal & Mobile app)	L1	1 to 3 years	Diploma/Engineering Graduate/Science Graduate. ▪ Good Communication (written/Oral) ▪ Good hands on experience on the technology used in the development of Portal and Mobile app etc ▪ Willing to work in 24X7 environment Should have worked in 1 similar project as L1
	L2	3 to 6 years	Diploma/Engineering Graduate/Science Graduate. ▪ Good Communication (written/Oral) ▪ Good hands on experience on the technology used in the development of Portal and Mobile app etc ▪ Willing to work in 24X7 environment Should have worked in 2 Similar Projects as L2.
Change Management Resources	L3	8 to 10 years	Diploma/Engineering Graduate/ Science Graduate. ▪ Good Communication (written/Oral) ▪ Having Minimum 5 years of experience on the technology used in the development of Portal and Mobile app etc ▪ Having strong documentation and SRS written skills

2.6.6 WARRANTY & ON-SITE MAINTENANCE

Hardware / Software Acceptance: - OICL will carry out the acceptance tests for testing of software, hardware and verification that the supplied components are as per bill of material. The Bidder shall assist OICL in all acceptance tests to be carried out by OICL. Bidder needs to rectify all the gaps highlighted in the Acceptance testing without any additional cost to OICL

Hardware / Software Go-Live: - The respective hardware and software will be termed as Go-live only when the application for which the hardware is allocated goes in production and all the data is migrated.

All the hardware (Infrastructure, OS, DB etc) will be hosted on the cloud as service so the bidder needs to factor the service cost from the day the Hardware is allocated to OICL in the cloud and connectivity is established.

The Bidder shall undertake to provide an onsite comprehensive 1 (One) Year Warranty and ATS for next 4 (four) years (BACK-TO-BACK with OEM) for all supplied Software commencing from the date of Go-Live and sign off by OICL of the software for the respective delivered locations of the Company as provided in the Purchase Order / Contract for Supply.

The Bidder will be single point of contact and responsible for AMC, ATS, guarantees & warrantees for all components, hardware, software, etc. Also, the facilities management should be available on-site and ensure adherence to SLAs. Bidder to note:

a. Warranties pertaining to Software / Applications, other Peripherals starts post Installation of the license at Production with the period of warranty as one year. ATS for Software/ Application shall begin post Completion of Warranty.

b. During FM period, Bidder will be responsible for:

   i. Overall maintenance and working of the Solution

   ii. Bug fixing and delivery of patches/ version changes effected

   iii. Creating knowledge repository for the bugs identified, resolution mechanism, version upgrade, future upgrade etc. of Application software, etc.

   iv. Provision should be available for version control and restoring the old versions if required by OICL

   v. Enhancement, modifications, customization, patches, upgrades due to statutory, regulatory, industry, changes till the SRS Sign off will be provided at no additional cost to OICL. During FM period, if due to any statuary and regulatory requirement, system requires any enhancement due to which there is major impact on sizing, then required procurement and delivery of hardware and software will be on mutually agreed terms and conditions. However, bidder has to provide all the services on CR basis to OICL.

   vi. Configuration changes, version up-gradations, performance monitoring, trouble shooting, patch installation, running of batch processes, database tuning, replacement/ support, technical support for application and data maintenance, recovery, query generation and management etc. of all software supplied under this RFP document.

   vii. Bug fixing should be undertaken in the event of software failure causing an interruption of operation of the proposed applications as per the response/ resolution times defined by OICL.

   viii. All the detected software errors must be notified and corrected, as per the agreed timelines

   ix. Provide OICL with monthly hardware utilization/performance monitoring reports and alert OICL in case of any performance issues by suggesting future capacity planning.

   x. The operational support staff should have support experience for Portal and Mobile app.

xi. Conduct DR drills in conjunction with the OICL's policies/procedures

c. Software/ Applications Delivery must coincide with cloud deployment.

Bidder has to deploy competent resources for the team to provide necessary maintenance and support as per the requirements of OICL. Bidder has to deploy adequate resources to ensure that the systems are up, and customer services are not impacted. To ensure that the SLAs are met, the Bidder, if required, will need to deploy additional resources during the contract period including implementation schedule without any additional cost to OICL. OICL has the right to interview and reject resources deployed by the Bidder.

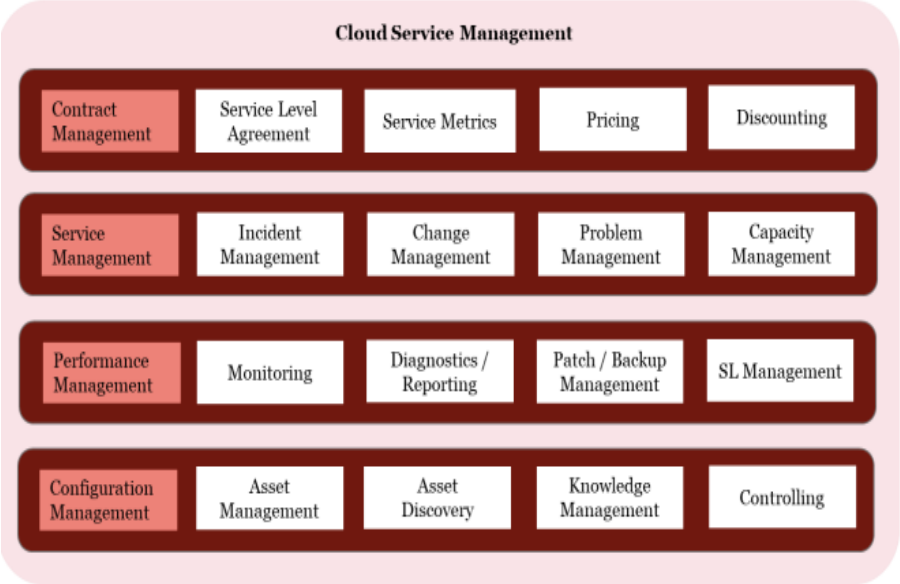
Bidder has to also ensure availability of resources spanning across all phases of implementation including Project Preparation, Solution Design, Configuration & Customization, Integration, UAT and Training. Bidder is required to right size and factor in adequate support and L1 & L2 Resources as part of Annexure 16 - Bill of Material to meet the Service Levels and Scope defined in the RFP.

The successful bidder shall not change any member of the project team during the course of the project without written consent from OICL.

Cloud Management Platform-

Cloud Management Platform (CMP) would be the centralized access point to manage Cloud deployments and would act as an interface to provision cloud-based IT Services. CMP may provide facility to manage the deployment and operation of applications and associated datasets across cloud service infrastructures. CMP may also provide management capabilities for both Native cloud. OICL requires a feature which allows to provision, manage, and terminate cloud services themselves through a Web portal or programmed service API calls. CMP is such a feature, a well-coordinated unified management framework that provides an interconnected view of the infrastructure and end-to end visibility. The Cloud management services provides the key capabilities which are necessary for operations and management of the resources and services required by the consumer. Cloud Management ensure smooth process flows as per business agreement and the prime objective is to maintain critical services up and running. Cloud management comprises of the administrative tasks involved with creation, maintenance, product/service performance and quality control of the environment within defined scope of work. Cloud management services focuses on processes and services invoked, such as when and where activities occur, who delivers them and how many people or entities they reach. OICLs should have the ability to create monitors that actively check various metrics, integration availability, network endpoints, and more. Following are some the most widely

used but not limited to cloud management services:



3 Terms & Conditions

3.1 General

3.1.1 Definitions

OICL/ PURCHASER: 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 www.orientalinsurance.org.in.

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

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

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

3.1.2.4. 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 fax or in electronic mail format or hardcopy letter, at the sole discretion of OICL.

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

3.1.2.5. **Preliminary Scrutiny** – OICL will scrutinize the offer to determine whether it is complete, whether any errors have been made in the offer, whether required technical documentation has been furnished, whether the documents have been properly signed,

and whether items are quoted as per the schedule. OICL may, at its discretion, waive any minor non-conformity or any minor deficiency in an offer. This shall be binding on the Bidder and OICL reserves the right for such waivers and OICLs decision in the matter will be final.

3.1.2.6. **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.

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

3.1.2.8. **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.

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

3.1.3 Sub-contracts

Sub-contracting is not allowed under the RFP. In case sub-contracting any of the activities under the scope of this RFP is required, the bidder needs to notify and take prior permission in writing from OICL. It is clarified that notwithstanding the use of sub-contractors by the Bidder, the Bidder shall be solely responsible for performance of all obligations under the RFP irrespective of the failure or inability of the subcontractor chosen by the Bidder to perform its obligations. The Bidder shall also have the responsibility for payment of all dues and contributions, as applicable including any statutory requirement and compliance. No additional cost will be incurred by OICL on account of sub-contract, if any.

3.1.4 Acceptance of the Solution

3.1.2.10. The User acceptance test will be carried out by the OICL team or consultant or PMO resources as per Acceptance Test Plan (ATP) against the bill of material and systems requirements. The system will be considered accepted (supplied, installed and operationalized) only after Acceptance Test is completed .

Some of features required to be completed are enumerated below:

i. The solution should correspond to what is stated in the purchase order without deviation except where mutually agreed upon

ii. The equipment is fully installed, commissioned and operational. The features specified in the Functional Specifications / mutually agreed for implementation should be demonstrated.

iii. The final acceptance of the system will be based on successful processing under live demonstration.

iv. First acceptance will be after equipment is installed, commissioned, tested and all features are demonstrated at the specified locations.

3.1.4.1. In case of discrepancy in hardware & related software supplied & not matching the Bill of Materials or technical proposal submitted by the bidder in their technical bid, the bidder shall be given 6 weeks' time to correct the discrepancy post which OICL reserves the right to cancel the entire purchase contract and the Bidder should take back their equipment at their costs and risks. The test will be arranged by the Bidder at the sites in the presence of the officials of OICL and/ or its consultants and appropriate functional and technical training should be given to the officials of OICL/ or its consultants. The warranty for all the software and other peripherals equipment & software by the Bidder pursuant to this Agreement will commence after go-live of the respective application. There shall not be any additional charges for carrying out this acceptance test. OICL will take over the system on successful completion of the above acceptance test. The Installation cum Acceptance Test & Check certificates jointly signed by Bidder's representative and OICL's official or its authorized representative should be received at Head Office along with invoice etc. for scrutiny before taking up the request for consideration of payment.

3.1.5 Conditional bids

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

3.1.6 Submission of Bids

Bidders shall submit the Bids online. For details please refer RFP Section 5 – Instruction to Bidders.

3.1.7 Performance Security

Within 15 days after the receipt of Notification of Award from OICL, the bidder shall furnish performance security to OICL as per Annexure - 6, which shall be equal to 3 percent (3%) of the value of the contract - valid till date of expiry of five year Contract period in the form of a bank guarantee from a nationalized/ scheduled bank as per the norms laid by the RBI.

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

3.1.8 Pre-Bid Meeting

All queries/ requests for clarification from bidders must reach us by e-mail (tender@orientalinsurance.co.in) or in person as per timeline given in section 1.4. 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.

3.1.9 Installation and Implementation

The bidder shall be responsible for supply, installation and commissioning of the proposed solution, hardware with technical specification as mentioned in Annexure-15 functional & Technical Specifications; and to undertake support of the same.

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

3.1.10 Delay in Bidder's performance

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

Any unexcused delay by the bidder in the performance of his implementation/service/other obligations shall render the bidder liable to any or all of the following sanctions: forfeiture

of his performance security, imposition of liquidated damages, and/ or termination of the contract for default.

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

3.1.11 Payment terms

The Bidder must accept the payment terms proposed by OICL. The financial 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.

Hardware, Software and other components to be provided for execution of project should be sized for entire contract period by considering Scope, functional & technical requirements and SLAs.

However, if it is found that the hardware is not sized adequately or the hardware utilization goes beyond the threshold limit as defined in the RFP, the Bidder has to provide additional hardware at no additional cost to meet the performance parameters set by OICL. The Bidder must accept the payment terms proposed by OICL as proposed in this Section. The financial offer 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.

The scope of work is divided in different areas and the payment would be linked to delivery and acceptance. All / any payments will be made subject to compliance of Service Levels defined in the RFP document. The 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 for the Supply of required Cloud, Software , Design, Installation, Implementation, and Commission of the solutions shall be made by OICL as per the solutions in scope as mentioned in the Scope of Work.

S.No.	Deliverables	% of Payment	STAGES (On completion of the activities)
1.	FM Support (as applicable)	Quarterly in arrears	Payment will be made quarterly in arrears. Bidder to submit the relevant documents with the attendance sheet along with the invoice
2.	ATS	Yearly in advance	Payment will be made post warranty period
3.	Training	100%	100% cost would be payable post successful completion of the training to the designated officials
4.	Cloud Charges (Infra, OS, DB etc) and application provided as service like (APM, ADR, API Gateway)	Quarterly in arrears	Payment will be made at the end of each quarter based on the usage of the service and as per the costs quoted in the Bill of Material
5	Benchmarking	50%	On submission of the Benchmarking Report
		50%	On Sign off the Benchmarking report by OICL
6	External Agency for testing	30%	On testing the base version and submitting the gap analysis
		30%	On testing and submission of test report on customized solution
		40%	On sign off and release to production
7	Data Migration Audit	40%	Submission of Pre-Migration Report
		60%	Submission of Post Migration Report
8	3rd party Audit	50%	On submission of the Report
		50%	On Sign off the report by OICL
9	Chatbot and Password less Authentication Licenses	70% of Software License cost of Respective application	Delivery of Base version of respective application software and on submission of Invoice and proof of Delivery.
		20% of Software License cost of Respective application	On UAT sign off for respective applications / module
		10% of Software License cost of Respective application	On successful release of customized software to production, for respective applications / module
10	Chatbot and Password less Authentication implementation	70% of Implementation cost for respective application	Go-live of respective application / module
		30% of Implementation cost for	One month after successful completion of respective application / module and on submission of Invoice and proof of completion

S.No.	Deliverables	% of Payment	STAGES (On completion of the activities)
		respective application	
11	Portal and Mobile app development and implementation	20% of implementation cost for Portal and Mobile app	SRS Sign off by OICL
		20% of implementation cost for Portal and Mobile app	UAT completion of Phase 1
		40% of implementation cost for Portal and Mobile app	Go-Live of Phase 1
		30% of implementation cost for Portal and Mobile app	Go-Live of Phase 2

OICL shall pay each undisputed invoice raised in accordance with this RFP and subsequent agreement, within thirty (30) Days after its receipt unless otherwise mutually agreed in writing, provided that such invoice is dated after such amount have become due and payable under this RFP and subsequent agreement.

Any objection / dispute to the amounts invoiced in the bill shall be raised by the OICL within 21 days from the date of receipt of the invoice, only in exceptional circumstances will OICL raise a dispute beyond 21 days. Upon settlement of disputes with respect to any disputed invoice(s), the OICL will make payment within thirty (30) Days of the settlement of such disputes.

3.1.12 Mode of Payment

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

3.1.13 Penalties and delays in Bidder's performance

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

3.1.14 Currency of Payments

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

3.2 Other RFP Requirements

a. The Head Office of OICL is floating this RFP. However, the Bidder getting the contract shall install and commission the solution, 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.

b. Technical Inspection and Performance Evaluation - OICL may choose to carry out a technical inspection/audit and performance evaluation of products 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.

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

d. OEM's Authorization Form – The Bidder should furnish a letter from original equipment manufacturer as mentioned in Annexure 12

e. Awareness and Training

Making OICL concerned Department aware about latest developments in the sector of cloud security would enable adopting the right set of tools, policies and procedures while deploying their application on cloud

f. Laws and Regulations

The Cloud Computing services would fall under the legal ambits of following legislations: Guidelines for Enablement of OICLs for Adoption of Cloud Management Office Page 95 of 99 • 'Cloud services' are recognized under the Integrated Goods and Services Tax Act 2017 (the GST Act) under 'online information and database access or retrieval services' and therefore the services rendered by Cloud Services Providers would be subject to GST. • Information Technology Act Section 43 A and the Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules 2011 (the Privacy Rules) under Information Technology Act provide guidelines for collection, use and protection of the sensitive personal data or information of persons by a body corporate that possesses, deals with or handles such data. • The IT Act and the Privacy Rules together set out the regulatory framework for creation, collection, storage, processing and use of electronic data (including personal and sensitive personal information recorded in electronic form) in India. • CSP's in India would also need to follow the principles of the Information Technology (Intermediaries Guidelines) Rules 2011 and (Intermediary Guidelines) under the Information Technology Act. • Government of India has drafted a Personal Data Protection Bill and the same once notified will overhaul the existing framework of privacy and data protection regime in India. The Bill is in many respects similar to General Data Protection Regulation, EU and it, inter alia, enhances the stringency of obligations and corresponding penalties governing data protection from a customer perspective. • In addition to the IT Act and Privacy Rules, the use of Cloud Computing in the banking and insurance sectors is subject to specific restrictions. The RBI's guidelines on Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks read along with the Report of Working Group of RBI on Electronic Banking set out specific requirements to be complied with by banks while engaging Cloud Service Providers. These requirements, inter alia, relate to vendor selection, data security, form of agreement, business continuity and disaster recovery or

management practices. • The Insurance Regulatory and Development Authority of India's (IRDAI) Guidelines on Information and Cyber Security for Insurers require insurers to comply with requirements, inter alia, in relation to data, application and network security, incident management, and information security audit while using services from a Cloud Service Provider. , also the Webapplication hosted on the cloud has to comply ISNP and ISMS standards or any other regulation proposed in future • On August, 24th, 2017, a nine-judge bench of the Supreme Court of India conclusively held that the right to privacy is a fundamental right guaranteed to the citizens of India (subject to reasonable restrictions). • The government retains the authority to intercept any information transmitted through a computer system, network, database or software for the prevention of serious crimes or under grave circumstances affecting public order and national security. The Ministry of Home Affairs has passed an order "authorizing" ten central agencies under Section 69(1) of IT Act, 2008, read with Rule 4 of IT Rules, 2009, for the " ……purposes of interception, monitoring Guidelines for Enablement of OICLs for Adoption of Cloud Cloud Management Office Page 96 of 99 and decryption of any information generated, transmitted, received or stored in any computer resource…"

g. Responsibilities of CSP for Infrastructure as a Service (IaaS):

The CSP shall be responsible for managing and controlling the underlying Cloud infrastructure including compute, operating systems, storage, network, security, etc. The indicative list of responsibilities of CSP for IaaS Cloud Service Model is as follows: - a. Provide Compute, Storage, hypervisors, network interfaces and other fundamental compute resources b. Provide redundancy and high availability for the IT infrastructure (IT Hardware – compute, network, storage, security) to meet the guidelines and SLA terms as laid down by MeitY. c. Provide auto-scalable, redundant and dynamic computing capabilities for virtual machines created as a part of the provisioned infrastructure. Provide interoperability support with regards to available APIs, data portability etc. Provide self-service tools to the OICLs that can be used to manage their Cloud infrastructure environments (v) Network Port Connectivity: Ensure network port connectivity for links between the OICL location(s)/Infrastructure and other Cloud environments (DC/DR) (vi) Tools: Provide relevant tools and services for backup, migration and replication of data, application and associated Databases (vii) Security: Ensure appropriate physical and logical security controls for Cloud deployment and service models as envisaged by MeitY (viii) Patch Management: Upgrade, maintain and deploy patches for underlying infrastructure and related components on cloud (ix) Disaster Recovery: Offer DR Services meeting DR requirements of the OICL in consonance to the guidelines laid down by MeitY (x) Cloud Access Logs: Provide authorized access to logs of all user activity within an account and the recorded information including API details, etc. (xi) Data Privacy: To ensure data privacy guidelines as defined by MeitY or OICL Department or Govt. of India are met by the CSP/MSP as applicable during the migration and other Cloud related activities (xii) Exit Management: To provide support to the OICL in case of Cloud to Cloud migration, for transferring data & applications, its associated databases, at the time of exit management and in line with the guidelines defined by MeitY. (xiii) Compliances: To ensure all the compliances as defined by MeitY for empanelment of Cloud Services offered by CSP and the security guidelines as defined by STQC. (xiv) Audit Support: Provide support during Audit by STQC / MeitY empaneled agency

or any agency appointed by the OICL Department.

h. Responsibilities of System Integrator / Implementation Agency

- This section lists down the indicative responsibilities of System Integrator whose services are being procured by the OICL. The responsibilities specific to a System Integrator include but not limited to are specified as below: - (i) Requirement Gathering: Gathering requirements, including business, system and functional, from the OICLs (ii) Requirement Mapping: Map key functional and non-functional requirements with the optimal solutions offered by the CSP (iii) Design & Develop: Design and Develop application(s) / software(s) to meet OICL needs / requirements (iv) Capacity Sizing: Conduct Capacity Sizing and planning for applications (v) Application Lifecycle: Build, Test and Deploy applications for the OICL on the CSP platform (vi) Integration Services: Provide integrations services for applications as per the requirement (vii) Test Plans: Executing Test plans to test application functionality (viii) Change Requests: Provide services specific to change requests raised by the OICL (ix) Patch Management: Upgradation and patching of application, it's database and maintenance (x) Support Services: Providing application support in case of any technical error or glitch (xi) Any other requirement as specified by the OICL. To provide Documentation and Release Management by performing functional testing through STQC , performance testing through STQC, to provide well documented development & testing process artifacts, To provide the following also Business Requirements Document (BRD) , Functional Requirement Specifications (FRS),Software Requirement Specifications (SRS) ,Software Design Documents (including HLD, LLD etc.) , Requirements Traceability Matrices (RTM) , Test Plan, Test Cases & Test Reports ,Code Review Reports (xii) Database Review Reports, Project Implementation Plan User Manual ,Deployment Guide. To provision convenient migration policies, for switching to alternative PaaS/IaaS provider to prevent vendor lock in the Managed Service Provider/SI must provide managed services for various components on the cloud as per the scope of work finalized and the MSP must share relevant reports with the OICL periodically as per the scope of work signed off between OICL and the MSP/SI. The OICL shall ensure that the CSP/ MSP/SI may perform the following tests post migration: • Infrastructure testing - various testing procedures including infrastructure (server, storage and network infrastructure) provided on Cloud. • VM testing o Storage/Disk IO testing. • Network throughput and latency testing • CPU and RAM benchmarking testing o Read/Write latency testing • Data Replication Testing • Firewall policy and configuration testing • Data Integrity Testing • Reverse Replication Testing • Switch over testing

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 five (5) year (Extendable for Two year on mutually agreed terms and conditions).

4.2 Ownership, Grant and Delivery

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

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

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

4.3 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.

4.4 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 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.

4.5 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.

4.6 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.

4.7 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

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

The Bidder shall not indemnify OICL for

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

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

4.8 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.

4.9 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.

4.10 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.

4.11 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.

4.12 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.

4.13 Technological Advancements

The hardware and software proposed as part of this contract

a. should not reach end of support during the period of contract
b. should not have been announced End of Life /Sales 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.

4.14 Confidentiality

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

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

a. possessed by Bidder prior to receipt from OICL, other than through prior disclosure by OICL, as documented by Bidder's written records;
b. published or available to the general public otherwise than through a breach of Confidentiality; or
c. obtained by Bidder from a third party with a valid right to make such disclosure, provided that said third party is not under a confidentiality obligation to OICL; or
d. Developed independently by the Bidder.

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

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

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

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

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

4.15 Guarantees

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

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 1% (One percentage) 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 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, Components 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.

4.18 Force Majeure

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

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

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

4.19 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.

4.20 Termination for Convenience

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

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

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

4.21 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.

4.22 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.

4.23 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)

4.24 Prices

The prices quoted (as mentioned in Appendix 2 - Bill of Materials submitted by the Bidder) for the solution and services shall be firm throughout the period of contract and shall not be subject to any escalation.

4.25 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.

4.26 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.

4.27 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 Supplier are made in full.

4.28 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. 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 Warranty, the bidder shall repay all the payment received from OICL and remove the solution supplied and installed by the bidder without any extra cost to the Company. If the Contract is cancelled during AMC, OICL shall deduct payment on pro-rata basis for the unexpired period of the contract

4.29 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.

4.30 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.

4.31 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.

4.32 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.

4.33 Repeat Order

OICL may place Repeat Order against the original order for a quantity up to 25% of the original order quantity during the contract period.

4.34 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 14.

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

4.35 Intellectual Property Rights

The code written by the bidder for Portal and Mobile app as pe the requirement and SRS Finalize for the scope of this RFP will be the Intellectual Property of the OICL. Bidder cannot use the same code for any other purpose. Bidder needs to submit the code to OICL with proper documentation as mentioned below after deployment.

- Data Flow Diagram
- Requirement traceability Matric
- Flow Diagram of different module
- Detail of technology used
- All the source code with proper documentation.

4.36 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, IRDAI 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.

4.37 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. You 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 you. 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, you 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) your use of and access of our page; (ii) your violation of any of these Guidelines; (iii) your 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.

4.38 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 solution as in totality which is the core element to provide services to the customer the entire order will go to the MSME vendor in the above-mentioned case.

As per the Government guidelines circular No 1(2)(1)/2016-MA Dated 10th March 2016 the eligibility criteria of Turnover and experience i.e point number 2, 3, and 9 of Section 1.6 is been relaxed for MSME after submission of valid certificate

4.40 Instruction for Online Bid Submission

- Bidders should comply to rules and regulations of GeM portal for submission of Bids online.
- However, bidder needs to submit following signed and stamped documents in **Hard Copies** in **four separate sealed** envelopes:-

    1. **Bill of Material as per format mentioned in Annexure 16.**
    2. **Non-Disclosure Agreement (NDA) as per format mentioned in Annexure 13**
    3. **Integrity Pact as per format mentioned in Annexure 14**
    4. **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 Ref No.& Date duly signed and stamped. If bidder does not submit the same, then bidder will be disqualified.
- The Sealed enveloped 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.

4.41 Procurement through Local Suppliers (Make in India)

Procurement through Local Supplier (Preference to Make in India) will be done as per the "Public Procurement (Preference to Make in India) Order 2017 issued vide Department of Industrial Policy and Promotion (DIPP) Notification No. P-45021/2/2017-B.E-II dated 15.06.2017 and thereafter revised vide Notification No. P-45021/2/2017-PP (B.E-II) dated: 28.05.2018 & No. P-45021/2/2017-PP(BE-II) dated 04.06.2020. Please also refer to Notification No. F.No.33(1)/2017-IPHW dt:14.09.2017 for the list of Electronic Products that are notified under the Public Procurement (Preference to Make in India) Order 2017.

'Local Supplier' means a supplier or service provider whose product or service offered for procurement meets the minimum local content as prescribed under this Order. The minimum local content shall be 50%.

The bidder (if local supplier) will have to submit a self-certification that the offered item meets the minimum local content and shall give details of the Locations at which the local value addition is made.

The bidder will also submit a certificate from statutory auditor or cost auditor of the company or from a practicing cost accountant or chartered accountant giving the percentage of local content.

5 Instruction to Bidders

- Bidders should comply to rules and regulations of GeM portal for submission of Bids online.
- However, bidder needs to submit following signed and stamped documents in **Hard Copies** in **four separate sealed** envelopes:-

    1. **Filled Bill of Material as per format mentioned in Annexure 16**
    2. **Non-Disclosure Agreement (NDA) as per format mentioned in Annexure 13**
    3. **Integrity Pact as per format mentioned in Annexure 14**
    4. **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 Ref No.& Date duly signed and stamped. If bidder does not submit the same, then bidder will be disqualified.
- The Sealed enveloped 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.

5.1 Tender Bidding Methodology

Sealed Bid System.

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

1. Eligibility & Technical Bid
2. Commercial Bid

5.2 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."

3. 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. No Blacklisting Declaration as per Annexure 2.
4. The corporate profile of the bidder (printed corporate brochure is preferred).
5. Bid Security Declaration as per Annexure 5
6. Statement of No-Deviation as per Annexure 7
7. Office and service infra declaration as per Annexure 8
8. The profile of the bidder (as per Annexure-9)
9. Bidder shall submit PAN number, GSTIN.
10. Annexure 11
11. Annexure 12
12. NDA (Annexure 13 on stamp paper)
13. Integrity Pact (Annexure 14 on Stamp Paper)
14. The power of attorney or authorization, or any other document consisting of adequate proof of the ability of the signatory to bind the Bidder
15. Annexure 17
16. Annexure 18
17. Annexure 20 – Stack confirmation

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 Minimum Functional and Technical Specifications as per Appendix 15.
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 Annexure 16 – Bill of Materials in the RFP. The Masked Bill of Material shall include details of the Software (Name, Version Details, License Metrics etc.), Hardware (Name of the Equipment with OEM Make and Model, CPU, RAM, HDD, Cores etc.), Facility Management (Efforts of Bidder and OEMs) etc.
5. Project Team Profile as in format of Annexure 19
6. Implementation plan & warranty support

7. Support Plan
8. User Training Plan
9. Transition Plan

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 / corrigendum 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

Bidder needs to submit signed and stamped **Bill of Material as per format mentioned in Appendix-1** in **Hard Copy** in **separate** **sealed** envelope. Total Amount in bill of material should match with the total Amount mentioned in the GEM Portal.

The Commercial Bid should provide 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 figure and words.

The amount quoted on GEM Portal should be inclusive of GST while the amount quote on Hard copy (Appendix -1 Bill of material) shown be exclusive of GST. There should not be any other difference other than GST. If there is any other difference found the bid will be rejected.

6.4 Mandatory Documents required in Hard Copies (offline)

The bidder needs to submit following signed and stamped documents in **Hard Copies** in **four separate sealed** envelopes:-

1. **Bill of Material as per format mentioned in Annexure 16.**
2. **Non-Disclosure Agreement (NDA) as per format mentioned in Annexure 13**
3. **Integrity Pact as per format mentioned in Annexure 13**
4. **Power of Attorney on stamp Paper in offline mode to OICL Head office in a sealed envelope.**

Evaluation Criteria

The competitive bids shall be submitted in Two stages:

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

Normalization of bids

The OICL will go through a process of technical and commercial evaluation and normalization of the bids to the extent possible and feasible to ensure that bidders are on the same technical ground. After the normalization process, if the OICL feels that any of the bids need to be normalized and that such normalization has a bearing on the commercial bid; the OICL may at its discretion ask all the technically shortlisted bidders to resubmit the updated technical and commercial bids once again for scrutiny. The OICL can repeat this normalization process at every stage of technical submission till the OICL is reasonably satisfied. The bidders agree that they have no reservation or objection to the normalization process and all the technically short-listed bidders will, by responding to this RFP, agree to participate in the normalization process and extend their co-operation to the OICL during this process. The bidders, by submitting the response to this RFP, agree to the process and conditions of the normalization process. Any non-compliance to the normalization process may result in disqualification of the concerned bidder.

OICL may call for any clarifications/ additional particulars required, if any, on the technical/ commercial bids submitted. The bidder has to submit the clarifications/ additional particulars in writing within the specified date and time. The bidder's offer may be disqualified, if the clarifications/ additional particulars sought are not submitted within the specified date and time. OICL reserves the right to call for presentation(s), product walkthroughs, on the features of the solution offered etc., from the bidders based on the technical bids submitted by them. OICL also reserves the right to conduct reference site visits at the bidder's client sites. Based upon the final technical scoring, short listing would be made of the eligible bidders for final commercial bidding.

6.5 Eligibility Evaluation

Eligibility criterion for the Bidders to qualify this stage is clearly mentioned in Clause 1.6. The Bidders who meet ALL these criteria and submit all the document as mentioned in the section 6.1 would only qualify for the second stage of evaluation. The Bidder would also need to provide supporting

documents for eligibility proof. All the credentials of the Bidder necessarily need to be relevant to the Indian market.

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

6.6 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:

Parameters	Percentage Weightage	Maximum Marks	Minimum Marks
Bidder Credentials	30%	300	150
Technical & Functional Specification Evaluation	50%	500	500
Manpower Credentials (Quality of Manpower Proposed)	15%	150	110
Bidder Technical presentation (Overall Solution Presentation)	5%	50	40
Total		1000	800

Bidders scoring at-least the minimum score in each section as mentioned in the table above and an overall score of 800 marks or more will be declared technically qualified.

The bidders scoring less than 800 marks (cut-off score) out of 1000 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. Bidder fulfilling the parameters stated above shall be considered as technically qualified. Once the evaluation of technical proposals is completed, the bidders who score more than the prescribed cut-off score will be shortlisted for further tender process.

In case none of the participating bidders qualify on technical criteria by reaching or exceeding the cut off score of 800, then the OICL, at its sole discretion, may relax the cut-off score to a lower value, which, in any case, shall not fall below 70%. In case at-least two participants have not scored 70%, then the OICL reserves the right to cancel and go for retendering process. However, this would be at the sole discretion of the OICL.

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

S.No.	Technical Evaluation	Evaluation Methodology
1	Bidder Credentials Strengths **(300 Marks)**	The Bidder must have developed the Portal and Mobile app and Portal & app must be live and running as on the date of submission of this RFP and must be catering of atleast 30 lakhs transactions per year. • One BFSI/Government in India (150 Marks) • Two BFSI/Government in India (250 Marks) • Three or more BFSI/ Government in India (300 Marks)
2	Technical & Functional Specification Evaluation **(500 Marks)**	The Bidder is required to submit the compliance for Annexure 15-Technical & Functional Specifications. Bidders should score 100% in Compliance to Annexure 15. The total marks of the Annexure will be scaled down on a scale of **500 marks** **Note:** • Deviations and non-conformance to requirements in the RFP shall be penalized • Unreasonable scope limitations which defeat the purpose of this RFP shall lead to reduction in scores or even possibility of disqualification of the bidder. This will be at the sole discretion of the OICL
4	Manpower Credentials (Quality of Manpower Proposed) **(150 Marks)**	1) Proposed Program Manager / Service Delivery Manager should have >10 years of experience of Managing IT Infrastructure, Managed services (Servers, storage, database, networks, backup & restore, Quality Assurance, application and Helpdesk Management) engagements **(50 Marks)** • One BFSI/ Government in India **(40 Marks)** • Two BFSI/ Government in India **(45 Marks)** • Three or more BFSI/ Government in India **(50 Marks)** 2) Proposed Managerial Role (In- Charge of Cloud Infra and network) should have >8 years of experience of Managing IT Infrastructure, Managed services (Servers, storage, database, networks, backup & restore) engagements **(50 Marks)** • One BFSI/ Government in India (40 Marks) • Two BFSI/ Government in India (45 Marks) • Three or more BFSI/ Government in India (50 Marks)

S.No.	Technical Evaluation	Evaluation Methodology
		2) Proposed Managerial Role (In- Charge of Portal & Mobile app) should have >8 years of experience of Managing Portals & Mobile app engagements **(50 Marks)** • One BFSI/ Government in India (30 Marks) • Two BFSI/ Government in India (40 Marks) • Three or more BFSI/ Government in India (50 Marks)
3	Bidder Technical presentation (Overall Solution Presentation) **(50 Marks)**	The bidders of this RFP have to give presentation/ interactions before the panel of representatives of OICL on the methodology/approach, time frame for various activities, strengths of the bidders on such projects The technical competence and capability of the bidder should be clearly reflected in the presentation. If any short-listed bidder fails to make such presentation, they will be disqualified from the selection process. OICL will confirm the veracity of the claim in the presentation during the site visit and if not satisfied, bidder will be disqualified from the selection process. **(Maximum 50 Marks)** • Understanding of OICL's business and Operating environment **(5 Marks)** • Demonstration of organization capability for the proposed initiative **(5 Marks)** • Demonstration of value proposition offered in the bid which shall enable the success of the project **(5 Marks)** • Project timelines **(5 Marks)** • Detailed Solution Capability showcasing below • the Use of Open API **(10 Marks)** • Design of solution on vendor Neutrality **(10 Marks)** • Implementation of Auto Scaling **(5 Marks)** • Approach **(5 Marks)**

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

6.7 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 five (5) 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.

Bidders need to note that the Annexure 16 Bill of material with complete bifurcation of Price which is mentioned in GEM Portal (As a consolidate Price) needs to submit at OICL Office (address mentioned in RFP). This needs to be submitted with proper labelling, seal, sign and stamped.

Bidder needs 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 Annexure 16 - Bill of material has to be tally till 2 decimal places. If any discrepancy found that bid will be rejected.

7 Service Level Agreement

Bidder shall ensure compliance with the SLAs defined in the RFP. This section describes the service levels that has been established for the services offered by the bidder to OICL. The bidder shall monitor and maintain the stated service levels to provide quality customer service to OICL.

7.1 System Availability

System availability is defined as {(Scheduled operation time - system downtime)/ (scheduled operation time)} *100%, where:

- Performance for availability service level default would be measured on monthly basis.
- "Scheduled operation time" means the scheduled operating hours of the system for the year. All planned downtime would be deducted from the total operation time for the year to give the scheduled operation time.
- "System downtime" subject to the SLA mentioned in this RFP, means accumulated time during which the system is totally in-operable due to in-scope system or infrastructure failure, and measured from the time OICL and / or its customers log a call with bidder's help desk of the failure or the failure is known to bidder from the availability measurement tools to the time when the system is returned to proper operation.
- OICL has critical and key infrastructure of DC and DR to be monitored on a 24*7 basis.
- Uptime will be for each individual server.
- Response may be telephonic or onsite depending on the criticality and how the SLA stands as per this RFP.

If any one or more of the proposed components at DC, NDR or DR are down resulting in non-availability of OICL server hardware, then downtime will be calculated as mentioned in the below section.

7.2 Issue Criticality Classification

The classification strategy has been envisaged to prioritize problem resolution based on OICL's priorities rather than in an ad-hoc manner. Classification framework will help OICL and the bidder to develop a shared understanding of the issue at hand, as well as the anticipated response and resolution timelines.

In order to improve the accuracy of the classification of an issue, application specific performance thresholds have been defined based on two characteristics, as mentioned below:

Impact: Number of users getting affected by the issue

Availability: Uptime of the system, both, in absolute terms as well as percentage terms

Criticality Level	IT Infra Grouping
Critical Mean IT Infra at DC & DR	• infra (cloud, storage, database, backup appliance / software) • API Gateway, ADR, APM etc
Key	• Non production env
Significant	• Standalone server / Components
Individual	• Components like Hard disk , Memory etc.

- In case of a disaster at DC or DR drill, DR would be the primary site and then, infrastructure at DR shall be considered as Critical and penalty shall be computed accordingly
- If any hardware (server etc.) in High Availability (HA) mode or tape library fails while other is working with no impact on the availability of the underlying solution/application, in such a case, penalty shall be levied on the failed hardware. The failed hardware in HA mode should be replaced within 12 hours of the failure. If the bidder fails to meet the timeline, OICL shall levy a penalty at the rate of **1% of the product and services cost [Total Product & Service], for every 2 hours of delay thereof, on the failed hardware (server, tape library etc.)**
- If both the hardware components fail in HA mode, OICL shall levy penalty on the bidder for the service levels defaults, basis the service levels requirement mentioned here.
- For three (3) downtime occurrences within a stipulated time window of a calendar month, a sum equivalent to 1% of the product cost of the respective product would be levied as a penalty. This would be over and above the monthly service level default penalty.

7.3 Service Level Default

As mentioned above, Service Level measurement would be on monthly basis. Bidder's performance will be assessed against Minimum Expected Service Level requirements mentioned in the Availability measurement table.

An Availability Service Level Default will occur when, the bidder fails to meet Minimum Service Levels, as measured on a monthly basis, for a particular Service Level.

Availability: -

Will be calculated as below

Availability = (U - C - D)/ (U - C)

System Scheduled Uptime for servers (U)

Scheduled Downtime for servers (C)

Unscheduled Downtime for servers (D)

Service Level Description	Minimum Service Level	Measurement Tools	Cost Reference for the Contract Period
Availability of Critical Infrastructure and software	99.99%	Enterprise Management System	Product cost at DC + Installation cost at DC + AMC & ATS cost at DC
Availability of Key Infrastructure and software	99.3%	Enterprise Management System	Product cost at DR + Installation cost at DR + AMC & ATS cost at DR
Availability of Significant Infrastructure and software	99%	Enterprise Management System	Product cost of standalone server + Installation cost at standalone server + AMC & ATS cost of standalone server
Availability of Individual components not impacting availability of the server/solution infrastructure	96.7%	Helpdesk/Enterprise Management System	For every hour of delay thereof, penalty shall be levied at the rate of INR 5000

Infrastructure and application Support

Response comprises acknowledgement of the problem and an initial analysis of the underlying cause

Uptime - The amount of time that the system is available for normal use. (Do note that planned maintenance would also be classified as normal use.)

Critical Level	Response Time	Resolution Time
Critical Infrastructure and software (Severity 1)	15 Min	Within 30 Mins of call reporting

Key Infrastructure and software (Severity 2)	30 Min	Within 4 Hrs of call reporting
Significant Infrastructure and software (Severity 3)	45 Min	Within 6 Hrs of call reporting
Individual components not impacting availability of the server/solution infrastructure ((Severity 4)	1 hr	Within 8 Hrs of call reporting

Service Level Description	Measurement	Minimum Service Level	Measurement Tool	Penalty
Hardware Utilization	Reporting to the OICL if Hardware daily peak utilization levels of CPU, RAM, NIC and hard disk etc. exceeds 70% (Seventy Percent) at any given point of time during business hours. Each incident should not exceed 5 minutes, every part thereof will be a new incident.	100%	Manual / Tool	If less than 3 times: for every 0.5% drop in service level, Penalty of 1% of the respective Hardware Cost If more than 3 times in a quarter: Bidder will be responsible for replacing/ augmenting the hardware at no additional cost to the OICL within 3 months of exceeding the thresholds. Incase bidder fails to replace the hardware, LD of 1% of effected

				product cost will be lived for every week of delay or part thereof
Storage Utilization	Production storage utilization levels exceeds 80% (Eighty percent) at any given point of time and such incidents occurs for more than 3 times in a quarter. Each incident should not exceed 5 minutes, every part thereof will be a new incident	100%	Manual / Tool	If less than 3 times: for every 0.5% drop in service level, Penalty of 1% of the respective Hardware Cost If more than 3 times in a quarter: Bidder will be responsible for replacing/augmenting the hardware at no additional cost to the OICL within 3 months of exceeding the thresholds. Incase bidder fails to replace the hardware, LD of 1%of effected product cost will be lived for every week of delay or part thereof
Software Service Request	Percentage of Software Service Requests concluded (software installation, patches, bug fixes, errors) within defined	100% per instance	Manual / Tool	INR 5000 for every instance of delay

	timeframe/response-resolution window.			
Downtime for servicing	• Each planned down - time for system servicing (up gradation, bug fixing, patch uploads, regular maintenance etc.) will not be more than 4 hours. • This activity will not be carried out during business hours. • However, such activities which require more than 1 hour or required to be carried out during business hours, will be scheduled in consultation with OICL. In case, downtime exceeds the planned hours, the additional time taken for servicing will be considered for infrastructure or system downtime as per availability measurements table.	100% per instance	Manual / Tool	INR 5000 for every 1 hour of delay above the scheduled downtime
Modification (Customization/ Enhancements) resolution for Application software	Bidder to ensure that all modifications, enhancements reported by the OICL and mutually agreed with the bidder will be duly sized and resolved as per the defined timeframes	96%	Manual / Tool	Monthly AMC / ATS of the affected services

UAT Bug Resolution	Bidder is required to ensure that all bugs reported by testing team during UAT will be duly resolved within defined timeframe	96%	Manual / Tool	Monthly AMC / ATS of the affected services
Backup Success Rate	Bidder needs to maintain 100% backup success rate	100%	Manual / Tool	• INR 500 for every daily backup/backup restoration failure • INR 1000 for every weekly/monthly backup/backup restoration failure • INR 5000 for every quarterly backup/backup restoration failure • INR 10000 for every yearly backup/backup restoration failure
Backup Window	Bidder needs to maintain the backup window of 3 hr	100%	Manual / Tool	<= 1 instance - No Charges >1 Instance - INR 1000 for every additional instance of Backup default
Patch Management	Patch management solution should be functional at any given point of time, on 90% of the device/server /application/endpoints	Per Instance	Manual / Tool	Penalty of INR 25,000 for every instance of default provided the default is due to bidder/product
DR Drill	NO of successful DR Drill conducted by the bidder	100%	ADR Tool	Penalty of INR 1,00,000 for every instance of default

				provided the default is due to bidder/product
RTO and RPO maintenance	Maintenance of RTO and RPO as mentioned in the RFP	100%	ADR Tool	Penalty of INR 1,00,000 for every instance of default provided the default is due to bidder/product
Content Uploading and Content Removal	Within 4 hours from the requested time.	100%	Manual	Above 4 hours within 8 hours: 10,000 Above 8 hours: 50,000
Scalability : **Scalability refers to scalability in terms of resources vCPU, RAM, Storage space, bandwidth over and above that is provisioned.**	Scalability for each of the resources: For VM's, provision of additional vCPU & RAM depending upon the load on the VM, free resources like vCPU & RAM available in VM should always be more than 30% and as soon as the resource utilization crosses 70% then the additional resources in terms of vCPU & RAM in same VM instance or additional VM should be provisioned in less than 1 min. For Bandwidth: provisioned bandwidth should be scaled vertically or horizontally on real	100%	Measured with the help of monitoring tool to monitor the graphical representation of allocated and utilized resources.	<99.5% & >=99% (10% of the <<periodic Payment>>) < 99% (30% of the <<periodic Payment>>) *For each additional drop of 1% in performance below 99%, 10% of<<Periodic Payment>> will be levied as additional penalty

	time basis For Storage: Addition of storage will be a change activity and the additional storage space to be provisioned within 1 hours of request raised			
Time to Resolve - Severity 1	For Severity 1, 98% of the incidents should be resolved within 30 minutes of problem reporting	100%	SLA Reporting Tool	<98% & >=90% (5% of the <<periodic Payment>>) < 90% & >= 85% (10% of the <<periodic Payment>>) < 85% & >= 80% (20% of the <<periodic Payment>>).
Time to Resolve - Severity 2,3,4	95% of Severity 2 within 4 hours of problem reporting AND 95% of Severity 3 within 6 hours of problem reporting And 95% of Severity 4 within 8 hours of problem reporting	100%	SLA Reporting Tool	<95% & >=90% (2% of the <<periodic Payment>>) <90% & >=85% (4% of the <<periodic Payment>>) <85% & >=80% (6% of the <<periodic Payment>>)
Availability of Root Cause Analysis (RCA) reports for Severity 1 & 2		100%	Average within 5 Working days	5% of <<periodic Payment>>

Availability of the network links at DC & DR	Availability for each of the network links: >= 99.5%	100%	SLA Report	<99.5% & >=99% (10% of the <<Periodic Payment>>) < 99% & >= 98% (20% of the <<Periodic Payment>>) < 98% & >= 97% (40% of the <<Periodic Payment>>) *For each additional drop of 1% in performance below 97%, 10% of<<Periodic Payment>> will be levied as additional penalty

Database & Application Response Assessment

Service Level Description	Measurement	Minimum Service Level	Measurement Tool	Penalty
Database Response Assessment	End to End response time within DC (from the Core Insurance Application and Portal to the respective Database and back) should be <10 ms (mile seconds) during business hours	100%	Application Performance Tool	For each 0.25% drop in the service level during business hours, penalty would be @1% (One Percent) of the

				overall cost of the hardware in TCO.
Application response time	This is the time taken from submission of any request by end-user – to - response of the request to the end user Response time < 2 sec	100%	Application Performance Tool	For each 0.25% drop in the service level during business hours, penalty would be @1% (One Percent) of the overall cost of the hardware in TCO
Page Transition	Time taken for page transition Response time < 2 sec	100%	Application Performance Tool	For each 0.25% drop in the service level during business hours, penalty would be @1% (One Percent) of the overall cost of the hardware in TCO

Management, Reporting and Governance

Service Level Description	Measurement	Minimum Service Level	Measurement Tool	Monthly Cost
Program Manager and Service delivery Manager	No change in these resources for minimum 1 year from the contract date and maximum 2 changes in the complete contract term (*the Program Manager should not be rotated to other clients of the Service Provider under the contract period).	100%	Manual	INR 1,00,000 for each default beyond the agreed threshold

Staff transition period (Handover period)	As per below Mentioning staff transition period Program Manager and service Delivery Manager: - 60 days All Domain in Charge:- 45 days Other Staff: - 30 days	100%	Manual	Program Manager/Delivery Manager-Penalty shall be INR 30,000 for each week of default or part thereof Domain In-charge- Penalty shall be INR 25,000 for each week of default or part thereof Other Staff- Penalty shall be INR 10,000 for each week of default or part thereof
Resource availability	Attendance for support personnel, L1 and L2 engineers. (covers all the locations) Minimum attendance level on any day is 90% of agreed deployment.	No of days below minimum attendance level	Manual	Penalty shall be INR 5,000 for every 2% default or part thereof below the agreed threshold

Overall cap of all the penalties over the tenure of the contract will be 15% (Fifteen percent) of the contract value.

Service Levels will be applicable for the respective Hardware and Software once the Same is accepted and Go-live

7.4 Penalty Computation

In the event of Service Level Default, bidder shall pay OICL a penalty that will be computed in accordance with the following formula:

Monthly Service Level Default = Minimum Service Level (for a month) – Actual Service Level (for a month)

Total amount of penalty, bidder is obligated to pay OICL, shall be reflected on the invoice provided to OICL in the quarter, after the quarter in which the Service Levels were assessed. OICL shall be entitled to deduct the penalty amount from the amounts payable by OICL to the selected bidder as per the invoice.

Example:

Service Level Description	Measurement
The achieved availability of Server / Software has been measured to be 98% in an assessment month.	For this example, let's assume, monthly Availability Service level is of 99.95%; for availability of 98%, penalty invoked would be of 1.95% of total cost of products and services of the failed component Cost Reference for 5-year tenure Server equipment cost = INR 1 crores (approximately) Server equipment AMC cost = INR 30,00,000 (approximately) Total cost of product and services for a Server equipment = 1,30,00,000 As mentioned above, for Availability Service level default of more than 99.5% and less than 98%, a penalty of 2% would be levied of the total cost of products and services calculated above. Thus, 2% of 1, 30,00,000 i.e. INR 2,60,000.

7.5 Incident Matrix

Incident to be Reported within (If unresolved)	Escalation Hierarchy

2 Hours	Concern Officers of OICL
4 hours	Manager-IT & Chief Manager (OICL)
8 Hours	Deputy General Manager (IT) & Chief Manager IT
> 16 hours	General Manager-IT & Deputy General Manager IT

7.6 AT RISK AMOUNT

The quarterly At-Risk Amount ('ARA') shall be 15% of the estimated quarterly pay-out of the respective month. In case maximum penalty is imposed for more than two times in a year, OICL will impose an additional penalty of 5% of the quarterly charges and may consider termination of services.

Overall cap for penalties as per SLA and the Liquidated damages over the tenure of the contract will be 15% (Fifteen per cent.) of the contract value

7.7 Other Conditions

i OICL expects the Bidder to complete the scope of the project as mentioned in section 02 - scope of work of this document within the timeframe specified in Section 1.7 Project Timelines of this document. Inability of the Bidder either to provide the requirements as per the scope or to meet the timelines as specified would be treated as breach of contract and would invoke the penalty /LD clause.

ii Inability of the Bidder to provide services at the service levels defined would result in breach of contract and would invoke the penalty clause

iii Notwithstanding anything contained above, no such penalty will be chargeable on the Bidder for the inability occasioned, if such inability is due to reasons entirely attributable to the OICL.

iv The Bidder is required to provide and implement regular updates/upgrades/patches released by the OEM within the timelines as mutually agreed.

v If during the contract period, any equipment has a hardware failure on four or more occasions in a quarter, it shall be replaced by equivalent or higher new equipment by the bidder at no additional cost to OICL.

vi The right to levy the penalty is in addition to and without prejudice to other rights / remedies available to the OICL such as termination of contract, invoking performance guarantee and recovery of amount paid etc.

vii OICL reserves the right to recover the penalty from any payment to be made under this contract.

viii Performance measurements would be assessed through audits or reports, as appropriate to be provided by the Bidder e.g. utilization reports, response time measurements reports, ticket details and resolution time report etc. The tools to perform the audit will need to be provided by

the Bidder. Audits will normally be done on regular basis or as required by OICL and will be performed by OICL or OICL appointed third party

7.7.1 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.

iii Conflict of Interest

The Managed Service Provider shall furnish an affirmative statement as to the absence of, actual or potential conflict of interest on the part of the Managed Service Provider or any prospective subcontractor due to prior, current, or proposed contracts, engagements, or affiliations with the Purchaser. Additionally, such disclosure shall address any / all potential elements (time frame for service delivery, resource, financial or other) that would adversely impact the ability of the Managed Service Provider to complete the requirements as given in the application document / RFP.

iv Data Ownership

All the data created as the part of the project shall be owned by Purchaser without any exceptions.

v Compliance with IS Security Policy

The Managed Service Provider shall comply with the Purchaser's IT Policy & IS policy in key concern areas relevant to the Project, details of which will be shared with the finally selected Managed Service Provider.

vi Changes in Cloud Service Offerings

The Managed Service Provider shall inform the Purchaser, at least 3 months in advance, about the material changes that the Managed Service Provider is planning to implement in the Cloud Service being consumed by the Purchaser. (ii) The Managed Service Provider is not allowed to discontinue offering a Cloud Service that is being consumed by the Purchaser, unless it poses a security threat, during the entire duration of the project. If the Cloud Service Offering is being discontinued due to the security threats, the Managed Service Provider has to first get this Cloud Service Offering de-empaneled from MeitY as per the guidelines specified by MeitY and provide a 3 months' notice to the Purchaser.

8 Disclaimer

This RFP is being issued by OICL for inviting bids for providing hardware, software and Services. 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 DGM
The Oriental Insurance Company Limited.
IT Dept, 2nd Floor,
"ORIENTAL HOUSE", Head Office,
A-25/27, Asaf Ali Road,
New Delhi-110002

Application form for the Eligibility of the Bidder

Tender Ref. No. OICL/HO/ITD/WEBPORTAL/2022/01 Dated 31 May 2022

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: No Blacklist Declaration

To
The DGM
The Oriental Insurance Company Limited.
IT Dept, 2nd Floor,
"ORIENTAL HOUSE", Head Office,
A-25/27, Asaf Ali Road,
New Delhi-110002

Subject: Submission of No Blacklisting Self-Declaration for Tender Ref. No: OICL/HO/ITD/WEBPORTAL/2022/01 Dated 31 May 2022 "REQUEST FOR PROPOSAL (RFP) FOR Selection of Vendor for Supply, Installation, Implementation, development & Maintenance of Web Portal and Mobile app"

Dear Sir/Madam,

We do hereby declare and affirm that we have not been blacklisted/debarred by any Government Departments, Agencies or Public Sector Undertakings in India as on the date of submission of the tender for "REQUEST FOR PROPOSAL (RFP) FOR Selection of Vendor for Supply, Installation, Implementation, development & Maintenance of Web Portal and Mobile app"

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 and services should be provided by the Vendor viz., _____ and has accepted a bid by the Vendor for the supply of those software and services in the sum of _____ (Contract Price in Words and Figures) (hereinafter "the Contract Price").

NOW THIS AGREEMENT WITNESSETH AS FOLLOWS:

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

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

RFP Document and corresponding Amendments (Reference No: OICL/HO/ITD/WEBPORTAL/2022/01 Dated 31 May 2022)

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

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

Company Seal
Witness I

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

Signed, Sealed and Delivered for M/s _____ by its constituted Attorney

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

Company Seal
Witness II

Signature _____
Name _____
Designation _____
Address _____
Company _____
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 DGM
The Oriental Insurance Company Limited.
IT Dept, 2nd Floor,
"ORIENTAL HOUSE", Head Office,
A-25/27, Asaf Ali Road,
New Delhi-110002

Sir,

Reg: Tender Ref No: **OICL/HO/ITD/WEBPORTAL/2022/01 Dated 31 May 2022**

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

1) if I/We withdraw the Bid during the period of validity i.e.180 Days from the Bid due date; or

2) if I/We is/are awarded the Contract and fail to sign the Contract; or

3) if I/We fail to submit an unconditional and irrevocable performance security before the deadline defined in the request for bid documents; or

4) if I/We make any statement or enclose any form which turns out to be false, incorrect and/or misleading at any time prior to signing of contract and/or conceals or suppresses material information; or

5) if I/We fail to submit the requisite documents as per the tender specification; or

6) if I/We violate any of the provisions of the terms and conditions of this tender Specification 7) If I/We become technically qualified but did not take part in the Reverse Auction

8) if I/We does not submit a NO deviation certification in the same format and language as mentioned in the RFP

9) if I/We does not provide requisite clarification as per the time mentioned in the clarification mail

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 the .....day of.....

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

9.7 Annexure 7: Statement of No Deviation

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

Reference: Tender Ref No: **OICL/HO/ITD/WEBPORTAL/2022/01 Dated 31 May 2022**

Sir,

This is to confirm that we have submitted a no deviation bid and unconditionally accept all requirements, payment terms, integrity pact, SLAs, Scope and the terms and conditions as mentioned in the said RFP including all corrigendum/amendment floated by OICL. pertaining to Selection of Vendor for Supply, Installation, Implementation, development & Maintenance of Web Portal and Mobile app. Any assumption or exclusion submitted by us in the proposal which are contradictory to the RFP or subsequent corrigendum/amendment stands null and void.

Name: _____

Designation: _____

Date: _____

Signature: _____

Company Seal

9.8 Annexure 8: Office locations and service infrastructure facilities

Tender Ref. No. OICL/HO/ITD/WEBPORTAL/2022/01 Dated 31 May 2022

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/WEBPORTAL/2022/01 Dated 31 May 2022

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

Name: _____

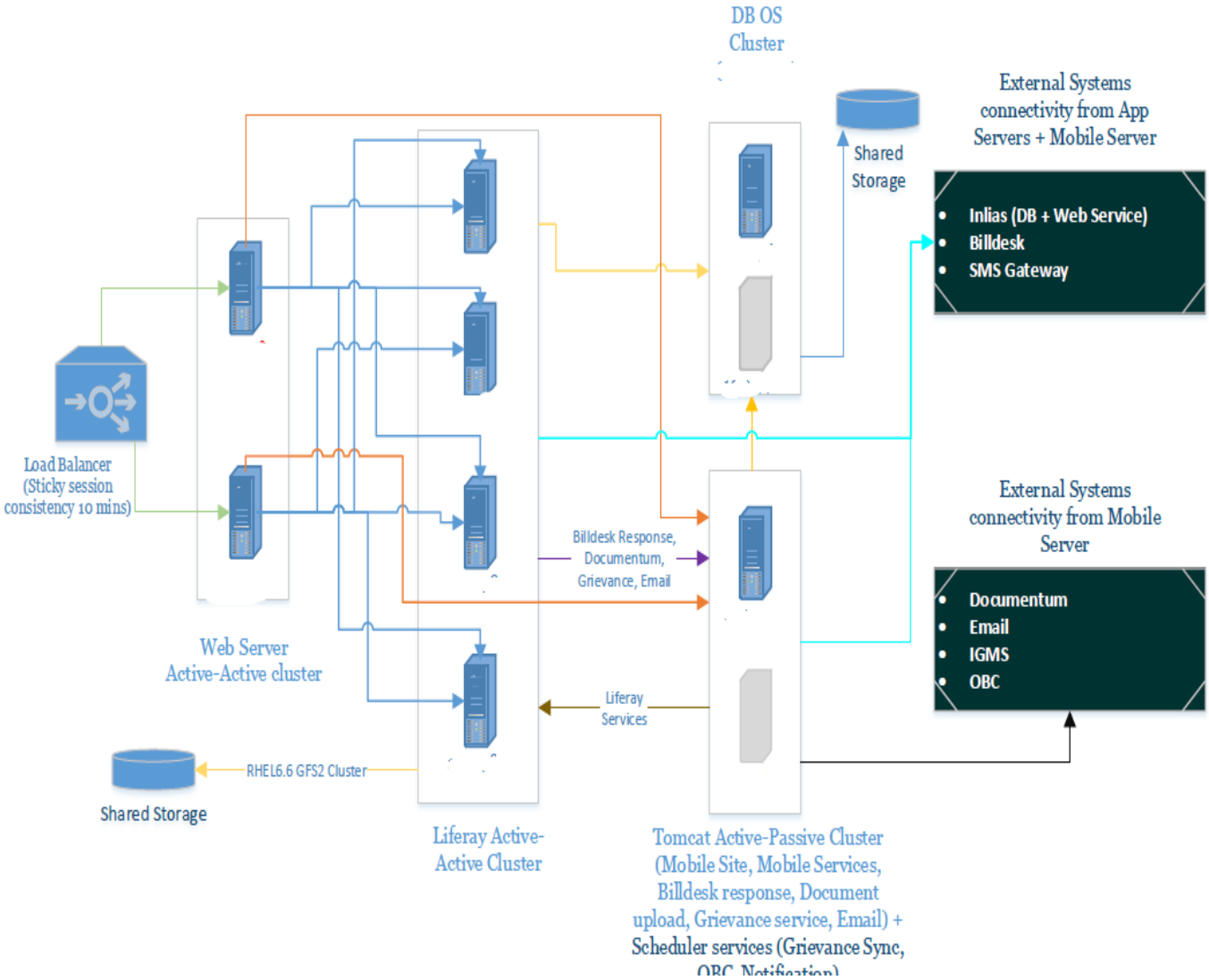
Designation: _____

Date: _____

Signature: _____

Company Seal

9.10 Annexure 10: OICL Present IT Setup



9.11 Annexure 11: Undertaking of Authenticity for Appliance and Equipment Supplies

RFP No: OICL/HO/ITD/WEBPORTAL/2022/01 Date:

To,

The DGM (IT)
Information Technology Department
The Oriental Insurance Company Limited 2nd Floor,
Head Office, Oriental House A-25/27, Asaf Ali Road,
New Delhi – 110 002

Dear Sir,

With reference to the Software Components 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, DB, licensed 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

9.12 Annexure 12: Manufacturers Authorisation Form

(To be submitted on OEMs Letter Head)

RFP No: OICL/HO/ITD/WEBPORTAL/2022/01 Dated 31 May 2022

To,

The DGM (IT)
Information Technology Department
The Oriental Insurance Company Limited 2nd Floor,
Head Office, Oriental House A-25/27, Asaf Ali Road,
New Delhi – 110 002

Subject: Manufacturers Authorisation Form for the "Tender for Proposal (RFP) for Selection of Vendor for Supply, Installation, Implementation, development & Maintenance of Web Portal and Mobile app**"**

<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. >
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, provided, that this option shall not relieve the Supplier 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.

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.

Name: _____

Designation: _____

Date: _____

Signature: _____

Company Seal

9.13 Annexure 13: 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 headquartered and Corporate Office at Oriental House, A-25/27, Asaf Ali Road, New Delhi - 110002 (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 continue till expiration of the Purpose or termination of this Agreement by The Oriental Insurance Company Ltd, whichever is earlier. 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)

9.14 Annexure 14: 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 Oriental House, A-25/27, Asaf Ali Road, New Delhi - 110002, 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. <u>Commitment of BIDDERS</u>

The BIDDERs commit itself to all take all measures necessary to prevent corrupt practices, unfair means and illegal activates 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 favour whatsoever during the tender process or during the execution of the contract.

4. <u>Previous Transgression</u>

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. <u>Earnest money (security deposit)</u>

5.1 While submitting commercial bid, the BIDDER shall deposit an amount_____(as specified in RFP) as Earnest money/security, with the BUYER through any of the following instruments:-

(i) Bank draft or a pay order in favor of _____

(ii) A confirmed guarantee by an Indian nationalized bank, promising payment of the guaranteed sum to the BUYER on demand within three working days without any

demur whatsoever and without seeking any reasons whatsoever the demand for payment by the BUYER shall be treated as conclusive proof of payment.

(iii) Any other mode or through any other instrument (to be specified in the RFP).

5.2 The Earnest money / Security deposit shall be valid up to a period of five years 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. <u>Sanctions for violations</u>

6.1 Any breach of the aforesaid provisions by the BIDDER or any one 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 consolation 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, including warranty period, whichever is later, 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: _____

9.15 Annexure 15: Functional and Technical Specifications

Annexure 15 is attached separately as excel which needs to fill and submit the same dully sealed

9.16 Annexure 16: Bill of Material

Annexure 16 is attached separately as excel which needs to fill and submit the same dully sealed and signed. Please note below :

The masked Bill of Materials which would be submitted as part of the Technical Bill of Material should contain "XX" for ALL the corresponding commercial values that will be present in the unmasked Bill of Material that will be part of the Commercial submission. The format of the Masked Bill material will be same.

9.17 Annexure 17: Land Border with India

To
The Deputy General Manager
The Oriental Insurance Company Limited.
IT Dept, 2nd Floor,
"ORIENTAL HOUSE", Head Office,
A-25/27, Asaf Ali Road,
New Delhi-110002

Subject: Offer for RFP Ref. No. OICL/HO/ITD/WEBPORTAL/2022/01 Dated 31 May 2022 "RFP for Selection of Vendor for Supply, Installation, Implementation, development & Maintenance of Web Portal and Mobile app"

Dear Sir/Madam,

I have read Office Memorandum F.No.6/18/2019-PPD dated 23.07.2020 issued by the Ministry of Finance, Department of Expenditure, Public Procurement Division inserting Rule 144 (xi) in GFRs 2017 which defines clauses regarding restrictions or procurement from a bidder of a country which shares a land border with India. I certify that _____(Bidder / OEM Name) is not from such a country or, if from such a country, has been registered with the competent authority, I certify that this bidder / OEM fulfils all requirements in this regard and is eligible to be considered. [Where applicable, evidence of valid registration by the competent authority shall be attached.]"

Signature:_____

Name: _____

Designation: _____

Date: _____

(Company Seal)

9.18 Annexure 18: Sizing Adequacy Letter

< To be submitted in the Bidder's letter head and should be signed by not below the company secretary>

To
The Deputy General Manager
The Oriental Insurance Company Limited.
IT Dept, 2nd Floor,
"ORIENTAL HOUSE", Head Office,
A-25/27, Asaf Ali Road,
New Delhi-110002

Subject: Offer for RFP Ref. No. OICL/HO/ITD/WEBPORTAL/2022/01 Dated 31 May 2022 "RFP for Selection of Vendor for Supply, Installation, Implementation, development & Maintenance of Web Portal and Mobile app"

Dear Sir/Madam,

We _____(Bidder Name & address) have reviewed the sizing submitted and in agreement with the proposed sizing to maintain the SLA for the contract duration . We confirm that the sizing is adequate and will meet the requirements of the OIC as stated in the RFP.

However, in the instance of the solution not working as per the SLA and response time mentioned in the RFP, we will augment the solution at no additional cost to the OICL

Signature:_____

Name: _____

Designation: _____

Date: _____

(Company Seal)

** In case of shortfall during the contract period then the bidder is required to provide the shortfall along with the following penalties.

Penalty would be levied as mentioned below:

a) Shortfall between 1% to less than 5% (cost of Hardware, Software, license in the BOM submitted at the time of bid) then penalty would be two times of shortfall
b) Shortfall between 5% to less than 10% (cost of Hardware, Software, license in the BOM submitted at the time of bid) then penalty would be three times of shortfall more than 10% (cost of Hardware, Software, license in the BOM submitted at the time of bid) penalty would be four times of shortfall

9.19 Annexure 19: Project Team Profile (Individual) Detailed

1	Name			
A	Brief Introduction (in bullets)			
2	Date of Birth			
3	Phone Number			
4	Position in the firm			
5	Total years of post-qualification work experience			
6	**Employment Record**			
	Company Name	Positions Held	Duration	**Clients Worked**
6.1				
6.2				
6.3				
6.4				
6.5				
7	Number of years the firm with			
8	**Details of relevant assignments undertaken (include both past and current employment projects and highlight BFSI experience, if any)**			
	(Provide scope, duration, client name and us of assignment) stat			
a	Year			
	Location			
	Client Name			
	Main project title and features			
	Position held			
	Activities performed			
b	Year			
	Location			
	Client Name			
	Main project title and features			
	Position held			
	Activities performed			
9	Education			
	Degree	**Year of**	**Institution**	

	Obtained	**Degree obtained**			
9.1					
9.2					
9.3					
9.4					
9.5					
10	Certification				
	Degree Obtained	**Year of Degree obtained**	**Institution**		
10.1					
10.2					
10.3					
10.4					
10.5					

9.20 Annexure – 20 Stack Confirmation

(Note:- Bidder needs to submit this letter on their letter head sully signed and stamp by Authorized signatory)

To
The Deputy General Manager
The Oriental Insurance Company Limited.
IT Dept, 2nd Floor,
"ORIENTAL HOUSE", Head Office,
A-25/27, Asaf Ali Road,
New Delhi-110002

Subject: Offer for RFP Ref. No. OICL/HO/ITD/WEBPORTAL/2022/01 Dated 31 May 2022 "RFP for Selection of Vendor for Supply, Installation, Implementation, development & Maintenance of Web Portal and Mobile app"

Dear Sir/Madam,

We hereby confirm that we have proposed below mentioned stack and there are no option quoted for any components

S.no	Component	OEM	Model / version
Portal Application			
Mobile application			
API gateway			
ADR			
APM			
Chatbot			
Password less Authentication			
Load balancer			
External testing Agency			

Data Migration Agency			
Benchmarking Agency			
Virtualization			
Operating System			
Server			
Cloud			
Database			
HSM & KSM			

Signature:_____

Name: _____

Designation: _____

Date: _____

(Company Seal)