Request for Proposal

For

Hiring of "Cloud based Disaster Recovery Services" from Managed Service Provider for SHCIL Services Limited

Tender Reference Number: SSL/19-20/IT/RFP-DR/001

Date of Issue: 21th August 2019

Tender document Amount: Rs. 5000/-

Issued By:

HEAD - IT & AUTO
SHCIL Services Limited, SHCIL House,
P-51, TTC Industrial Area, MIDC,
Mahape, Navi Mumbai 400710
Email: ssl.it@shcilservices.com

1. Disclaimer

This Request for Proposal (**RFP**) for "**Hiring of "Cloud based Disaster Recovery Services" from Managed Service Provider"** is issued by SHCIL Services Ltd (SSL)**.**

Whilst the information in this RFP has been prepared in good faith, it is not and does not purport to be comprehensive or to have been independently verified. Neither SSL nor any of its officers or employees, nor any of their advisers nor consultants accept any liability or responsibility for the accuracy, reasonableness or completeness of the information contained in the RFP, or for any errors, omissions or misstatements, negligent or otherwise, relating to the proposed Hiring of "Cloud based Disaster Recovery Services" from Managed Service Provider at different seismic zone for SSL setup (hereinafter referred to as "SSL Cloud Based DR"), or makes any representation or warranty, express or implied, with respect to the information contained in this RFP or on which this RFP is based or with respect to any written or oral information made or to be made available to any of the recipients or their professional advisers and, so far as permitted by law and except in the case of fraudulent misrepresentation by the party concerned, and liability therefore is hereby expressly disclaimed.

The information contained in this RFP is selective and is subject to updating, expansion, revision and amendment at the sole discretion of SSL. It does not, and does not purport to, contain all the information that a recipient may require for the purposes for making a decision for participation in this process. Each party must conduct its own analysis of the information contained in this RFP, to correct any inaccuracies therein and is advised to carry out its own investigation into the proposed SSL Project, the regulatory regime which applies thereto and by and all matters pertinent to the SSL Project and to seek its own professional advice on the legal, financial and regulatory consequences of entering into any agreement or arrangement relating to the SSL Project. SSL shall not be responsible for any direct or indirect loss or damage arising out of or for use of any content of the RFP in any manner whatsoever.

SSL shall be the sole and final authority with respect to qualifying a bidder through this RFP. The decision of SSL in selecting the Service Provider who qualifies through this RFP shall be final and SSL reserves the right to reject any or all the bids without assigning any reason thereof. SSL further reserves the right to negotiate with the selected Service Provider (SP) to enhance the value through this project and to create a more amicable environment for the smooth execution of the project.

SSL may terminate the RFP process at any time without assigning any reason and upon such termination SSL shall not be responsible for any direct or indirect loss or damage arising out of such a termination.

1.1 Abbreviations

Abbreviation	Description
B2C	Business to Consumer
BI	Business Intelligence
BKC	Bandra Kurla Complex
CMMI	Capability Maturity Model Integration
DC	Data Centre
DEV	Development
DR	Disaster Recovery
DSC	Digital Signal Certificate
EMD	Earnest Money Deposit
ETIM	Electronic Ticketing Machine
GCC	General Contract Conditions
GoM	Government of Maharashtra
ICT	Information Communication Technology
IT	Information Technology
ITB	Instructions to bidder
MIS	Management Information System
MSP	Managed Service Provider
NDA	Non-Disclosure Agreement
NIC	National Informatics Centre
PBG	Performance Bank Guarantee
PDF	Portable Document Format
PM	Project Management
QGR	Quarterly Guaranteed Revenue
RFP	Request for Proposal
RFP	Request for Proposal
SD	Security Deposit
SSL	SHCIL Services Limited
SLA	Service Level Agreement
TEC	Tender Evaluation Committee

1.2 Key Terms - Definition

Term	Definition
Bid / Proposal	This means the documents in their entirety comprising of the pre-qualification Proposal, Technical and Commercial Proposal, clarifications to these, technical presentation/ demo submitted by the Bidder, the Bidder herein, in response to the RFP, and accepted by SSL.
Bidder(s)	Eligible, reputed, qualified IT entities or Consortium of these with strong technical and financial capabilities for supply, design, customization, implementation, hosting and maintenance of ICT Solution who may be responding to this RFP.
Bidder's Representative	The person or the persons appointed by the Bidder from time to time to act on its behalf for overall co-ordination, supervision and execution of Project.
Business Day	This means any day that is not a Sunday or a public holiday (as declared by Government of Maharashtra).
Contract / Project Period	3 Years post Go-Live.
Day	A period of 24 hours running from midnight to midnight. It means "calendar day" unless otherwise stated. Where, because of a difference in time zone, the calendar day in one country differs from another country then the calendar day shall be deemed to be the calendar day applicable to India.
Deliverables	The documents, milestones and activities related to the setting up and operations of Project in SSL, as defined in the RFP.
EMD/ Bid Security	This refers to the amount to be deposited by the Bidders to SSL to demonstrate commitment and intention to complete the process of selection of Bidder for implementation of ERP in SSL.
End of Contract	This refers to the time when the Contract Period has ended.
RFP/ Tender	This means the Request for Proposal released, containing the technical, functional, commercial and operational specification.
Contract	This shall mean the deed to contract, together with its original accompaniment and those latter incorporated in it by mutual consent.
Contractor	This shall mean the successful Bidder whose tender has been accepted, and who has been authorized to proceed with the Work.
Subcontractor	This means person or corporate body who has a Contract with the Contractor to carry out a part of the Work in the Contract which includes work on the Site.
Employer	This shall mean SSL and is the party who will employ the Contractor to carry out the Works.
Users	This means the internal and external users of the System including citizens, business firms, SSL including its offices, corporations and agencies and their employees, as the context admits or requires

1.3 Tender Notice

TENDER NOTICE

Tender Reference No: SSL/19-20/IT/RFP -DR/001 **Date: - 21.08.2019**

SHCIL Services Ltd (SSL) hereby invites bids from eligible bidders for Hiring of "Cloud based Disaster Recovery services" from Managed Service Provider for SSL IT Setup. Last date for bid submission is **16.09.2019 till 3.30 pm**. For details, please refer tendering portal www.shcilservices.com/Tender Notices. For any assistance. Contact SSL IT official on 022-61778600 Timings-India 09.00 Hrs. – 17.30Hrs (GMT+5.30).

Date: 21.08.2019 SD

Place : Navi Mumbai HEAD - IT & AUTO, SSL

2. Invitation for Proposal

SSL hereby invites Proposals from reputed, competent and professional companies, who meet the Pre-Qualification Criteria as specified in this bidding document for **"Hiring of Cloud based Disaster Recovery services" from Managed Service Provider for SHCIL Services Ltd(SSL)"** as detailed in this RFP document.

All documents related to RFP is available on the SSL website portal www.shcilservices.com/TenderNotices. All bidders must note that this bids received only through sealed packets. To participate applicant / bidders is required to provide sealed packet proposals.

- Bidder may contact IT representative at (Ph. No. 022-61778600 / 7718805012) for any assistance. Contact Timings-India 09.00 Hrs. - 17.30Hrs (GMT +5.30)

Bidder/ Agencies are advised to study this RFP document carefully before submitting their proposals in response to the RFP Notice. Submission of a proposal in response to this notice shall be deemed to have been done after careful study and examination of this document with full understanding of its terms, conditions and implications. Prospective bidders are advised to check the minimum qualification criteria before participating in the bidding process. This RFP document is not transferable and the name of the bidder who purchases and submits the same bid shall be unchanged.

2.1 Key Events and Dates

The summary of various activities with regard to this invitation of bids are listed in the table below:-

#	Particular	Details
1.	Advertising Date	From: 21.08.2019
2.	Name of the project	RFP for "Hiring of "Cloud based Disaster Recovery services" from Managed Service Provider for SSL IT Setup SHCIL Services Ltd(SSL)"
3.	RFP Document Download and Submission Start Date & Time	From Date: 21.08.2019, Time 11:30 am Till Date: 16.09.2019, Time : 3.30 pm
4.	Website for downloading Tender Document, Corrigendum's, Addendums etc.	https://www.shcilservices.com/important-notices

5.	Last date for Submission of Queries	28.08.2019 at 3:00 pm All the queries should be received on or before, through email only with subject line as follows: "Pre-Bid queries - <Agency's Name>". The Pre-Bid queries to be sent to the Email Id – ssl.it@shcilservices.com
6.	Pre-Bid Conference	30.08.2019 at 3:00 pm Address: SHCIL Services Limited, SHCIL House, P-51, TTC Industrial Area, MIDC, Mahape, Navi Mumbai 400 710
7.	Last date (deadline) for Submission of bids	16.09.2019 till 3.30 pm
9.	Date and time for opening of Commercial bids	Will be intimated later to the qualified bidders
10.	Detail of the contact person and Address at which sealed bids are to be submitted	HEAD-IT & AUTO SHCIL Services Ltd. SHCIL House, P -51, TTC Industrial Area, Mahape, Navi Mumbai—400 710 E-mail: ssl.it@shcilservices.com

2.2 Other Important Information Related to Bid

#.	Item	Description
1.	RFP Document Fee to be paid via Demand Draft in favour of "SHCIL Services Ltd" only.	Rs. 5000 (Rupees Five Thousand Only) Non Refundable
2.	Bid Validity Period	One hundred and eighty (180) days from the date of opening of bid
3.	Last date for signing contract	As intimated in work order of SSL
4.	Contract Period	3 Years post Go-Live

Note: Prospective Bidders may visit SSL IT Office for any further information/clarification regarding this RFP on prior appointment during working hours till the date of technical bid submission.

3. Instructions to Bidders

3.1 Introduction of SSL

SHCIL Services Ltd Limited (SSL) is 100% wholly subsidiary of Stockholding Corporation of India Ltd.. SSL is broking arm of Stockholding and having membership with BSE, NSE, & MCX. SSL is running its business from its corporate office located at SHCIL House, P-51, TTC Industrial Area, Mahape, Navi Mumbai 400 710.

SSL has envisioned the development of DR site integrated IT enabled e-governance system across the organization in order to ensure transparent, easy, efficient and accurate availability of information, and facilitation of transactions. With intent of providing a robust system, SSL has decided to structure its current systems and core functions through e-governance solutions by leveraging Information and Communication Technology across various functions in the organization.

SSL has Core business (Trading & Back office) enterprise systems like ODIN and LD Back office which it plans to host on a Cloud Model for Disaster Recovery site as per regulatory norms and conditions.

3.2 Purpose

SSL seeks the services of from reputed, competent and professional Information Technology (IT) companies, who meet the Pre-Qualification Criteria as specified in this bidding document for the "RFP for Hiring of "Cloud based Disaster Recovery services" from Managed / Cloud Service Provider for IT setup of SHCIL Services Ltd". This document provides information to enable the bidders to understand the broad requirements to submit their bids. The detailed scope of work is provided in Section 4 of this RFP document.

Address for Correspondence & Contact Person:

HEAD – IT & AUTO
SHCIL Services Limited
SHCIL House, P – 51,
TTC Industrial Area,
Mahape, Navi Mumbai
Pin 400 710
E-mail: ssl.it@shcilservices.com

Consortium

The consortium or joint ventures are not allowed and only MSP are not allowed.

3.3 Sub-Contracting Conditions

1. The Bidder can sub-contract project activities only related to installation, commissioning configuring and maintenance of Connectivity from Cloud Service Provider to SSL. However, it is clarified that the Bidder shall be the principal employer for all claims arising from the

liabilities statutory or otherwise, concerning the sub-contractors. The Bidder undertakes to indemnify the Nodal Agency or its nominated agencies from any claims on the grounds stated hereinabove.

2. The bidder shall share all the details of the Service Provider in the Technical Bid. Both during the process of award, and post award of contract, if there is a change in subcontractor, the Bidder shall obtain prior permission from SSL.

3.4 Completeness of Response

1. Bidders are advised to study all instructions, forms, terms, requirements and other information in the RFP documents carefully. Submission of bid shall be deemed to have been done after careful study and examination of the RFP document with full understanding of its implications.
2. The response to this RFP should be full and complete in all respects. Failure to furnish all information required by the RFP document or submission of a proposal not substantially responsive to the RFP document in every respect will be at the Bidder's risk and may result in rejection of its Proposal.

3.5 Proposal Preparation Costs

1. The bidder shall submit the bid at its cost and SSL shall not be held responsible for any cost incurred by the bidder. Submission of a bid does not entitle the bidder to claim any cost and rights over SSL and SSL shall be at liberty to cancel any or all bids without giving any notice.
2. All materials submitted by the bidder shall be the absolute property of SSL and no copyright/patent etc. shall be entertained by SSL.

3.6 Bidder Inquiries

Bidder shall e-mail their queries at SSL.IT@Shcilservices.com e-mail address. No queries will be entertained thereafter. This response of SSL shall become integral part of RFP document. SSL shall not make any warranty as to the accuracy and completeness of responses.

3.7 Amendment of RFP Document

1. All the amendments made in the document would be published on the SSL website Portal and shall be part of RFP.
2. The Bidders are advised to visit the aforementioned website/portal on regular basis to check for necessary updates. The SSL also reserves the right to amend the dates mentioned in this RFP.

3.8 Supplementary Information to the RFP

If SSL deems it appropriate to revise any part of this RFP or to issue additional data to clarify an interpretation of provisions of this RFP, it may issue supplements to this RFP. Any such corrigendum shall be deemed to be incorporated by this reference into this RFP.

3.9 SSL's right to terminate the process

SSL may terminate the RFP process at any time and without assigning any reason. SSL reserves

the right to amend/edit/add/delete any clause of this Bid Document. This will be informed to all and will become part of the bid/RFP and information for the same would be published on the SSL website portal under Tender Notices.

3.10 Authentication of Bid

1. The original copy (hard copy) of the Bid Document shall be signed, stamped and submitted along with the bid. Authorized person of the bidder who signs the bid shall obtain the authority letter from the bidder, which shall be submitted with the Bid. All pages of the bid and its annexures, etc. shall be signed and stamped by the person or persons signing the bid.
2. Registered/ irrevocable Power of Attorney executed by the Bidder in favour of the duly authorized representative, certifying him as an authorized signatory for the purpose of this bid. In the case of the Board resolution authorizing a person as the person responsible for the bid, the Board resolution shall be submitted. The person accountable for the bid shall remain the full time employee of the bidder till the end of contract period.

3.11 Language of Bids

This bid should be submitted in English language only. If any supporting documents submitted are in any language other than English, then the translation of the same in English language is to be duly attested by the bidder and submitted with the bid, and English translation shall be validated at SSL's discretion.

3.12 Patent Claim

In the event of any claim asserted by a third party of infringement of copyright, patent, trademark or industrial design rights arising from the use of the goods or any part thereof, the bidder shall expeditiously extinguish such claim. If the bidder fails to comply and SSL is required to pay compensation to a third party resulting from such Infringement, the Bidder shall be responsible for such compensation, including all expenses, court costs, lawyer fees etc. SSL shall give notice to the Successful Bidder(s) of any such claim and recover it from the bidder.

3.13 Bid Submission Format

The entire proposal shall be submitted strictly as per the format specified in this Request for Proposal. Bids with deviation from this format are liable for rejection.

3.14 Bid Submission Instructions

Bidder has to submit bids in single envelope system containing two sealed pack envelops (1.Eligibility Criteria & Technical 2 Commercial). Submission of bids shall be in accordance to the instructions given in the Table below:

Particulars	Instructions
Envelope A:	Scanned copy of Receipt of the Tender Fees**.**
Technical Proposal	The Pre-qualification documents/ Eligibility and Technical documents shall be prepared in accordance with the requirements specified in this RFP and the formats are prescribed in this RFP. Bidders shall

Technical	submit accurately filled Checklist for Pre qualification documents and evaluation documents as per format in section 6.7 and section 6.8. Each page of the Technical Proposal should be signed and stamped by the Authorized Signatory of the Bidder. Technical Proposal should be submitted through online bid submission process only.
Particulars Instructions	
Envelope B: Financial Proposal	The Financial Proposal shall be prepared in accordance with the requirements specified in this RFP and in the formats prescribed in Section 7 of the RFP. Each page of the Financial Proposal should be signed and stamped by the Authorized Signatory of the Bidder. Financial Proposal should be submitted through online bid submission process only.

The following points shall be kept in mind for submission of bids;

1. SSL shall not accept open proposal.
2. The Bidder is expected to price all the items and services sought in the RFP and proposed in the proposal. The Bid should be comprehensive and inclusive of all the services to be provided by the Bidder as per the scope of his work and must cover the entire Contract Period.
3. SSL may seek clarifications from the Bidder on the Technical proposal. Any of the clarifications by the Bidder on the Technical proposal should not have any commercial implications. The Financial Proposal submitted by the Bidder should be inclusive of all the items in the Pre-Qualification proposal and should incorporate all the clarifications provided by the Bidder on the Pre-Qualification proposal during the evaluation of the Pre-Qualification offer.
4. Financial Proposal shall not contain any technical information.
5. If any Bidder does not qualify the prequalification criteria stated Section 3.23 of this RFP and doesn't meet minimum qualifying marks for technical evaluation , the financial proposals of the Bidder shall not be opened in the Tendering system.
6. It is required that the all the proposals submitted in response to this RFP should be unconditional in all respects, failing which SSL reserves the right to reject the proposal.
7. Proposals sent by fax/post/courier shall be rejected.

3.15 Late Proposal and Proposal Validity Period

Proposals received after the due date and the specified time (including the extended period if any) for any reason whatsoever, shall not be entertained and shall not be opened. The validity of the proposals submitted before deadline shall be till 180 days from the date of submission of the proposal.

3.16 Modification and Withdrawal of Proposals

No Proposal shall be withdrawn in the interval between the deadline for submission of proposals and the expiration of the validity period specified by the Bidder on the Proposal form. Entire EMD shall be forfeited if any of the Bidders withdraw their proposal during the validity period.

3.17 Non-conforming Proposals

A Proposal may be construed as a non-conforming proposal and ineligible for consideration:

1. If it does not comply with the requirements of this RFP.
2. If the Proposal does not follow the format requested in this RFP or does not appear to address the particular requirements of the SSL.

3.18 Acknowledgement of Understanding of Terms

By submitting a Proposal, each Bidder shall be deemed to acknowledge that he/she has carefully read all sections of this RFP, including all forms, schedules, annexure, corrigendum and addendums (if any) hereto, and has fully informed itself as to all existing conditions and limitations.

3.19 Bid Opening

1. Total transparency shall be observed and ensured while opening the Proposals/Bids
2. SSL reserves the rights at all times to postpone or cancel a scheduled Bid opening.
3. Bid opening shall be conducted in two stages.
4. In the first stage, Technical Envelope of proposals shall be opened and evaluated as per the pre-qualification and technical evaluation criteria mentioned in the RFP.
5. In the second stage, Commercial Proposals of those Bidders, who qualify Pre Qualification Criteria and Technical criteria, shall be opened. All Bids shall be opened in the presence of Bidders' representatives who choose to attend the Bid opening sessions on the specified date, time and address.
6. The Bidders' representatives who are present shall sign a register evidencing their attendance. In the event of the specified date of Bid opening being declared a holiday for SSL, the bids shall be opened at the same time and location on the next working day. In addition to that, if there representative of the Bidder remains absent, SSL will continue process and open the bids of the all bidders.
7. During Bid opening, preliminary scrutiny of the Bid documents shall be made to determine whether they are complete, whether required Bid Security has been furnished, whether the Documents have been properly signed, and whether the bids are generally in order. Bids not conforming to such preliminary requirements shall be prima facie rejected. SSL has the right to reject the bid after due diligence is done.

3.20 Evaluation Process

1. SSL shall evaluate the Tender Fee, EMD, Pre-Qualification documents and Technical Evaluation documents (Envelope A), and Financial Proposal (Envelope B) and submit its recommendation to the Competent Authority whose decision shall be final and binding upon the bidders.
2. Bidders shall be evaluated as per the pre-qualification and technical evaluation criteria mentioned in Prequalification criteria and Technical criteria. of the RFP.
3. Bidders with minimum technical score of 60 out of 100 in technical evaluation will be

considered to be eligible for financial evaluation

4. Amongst the bidders who are considered for financial evaluation, the bidder who has quoted the Least will be considered as most eligible for award, at the discretion of SSL. SSL, however reserves the right to accept or reject any or all bids without giving any reasons thereof.
5. The bidder shall provide required supporting documents with respect to the PreQualification Proposal, Technical Proposal evaluation as per the criteria mentioned in Prequalification and Technical Criteria of this RFP.
6. Please note that SSL may seek inputs from their professional, external experts in the Bid evaluation process.
7. In no way the bidder shall indicate its Financial Offer in any Envelope other than Envelope B. In case it is found, SSL may summarily reject the proposal of the said bidder.

3.21 Prequalification criteria

A. For Managed Service Provider (MSP) / Cloud Service Provider / Bidder

Sr. No.	Basic Requirement	Eligibility Criteria	Documents to be submitted
PQ1	Legal Entity	The MSP/CSP should be a company registered under the Companies Act, 1956.	Copy of Certificate of Incorporation/ Registration
			Copy of PAN Card
			Copy of GST Registration
PQ2	Turnover	The MSP / Bidder should have minimum average annual turnover of atleast Rs. 2.5 crore in India for the last three financial years (FY 16-17, FY 17-18, FY 18-19). If current financial year the Annual Turnover details is not available then CA certificate for provisional or unaudited turnover can be submitted.	Profit & Loss, Balance Sheet and Certificate Turnover Certificate from Chartered Accountant
PQ 3	Data Center Facility	The Data Centers should be at least Tier III standard, Certified under TIA 942 or Uptime Institute certifications.	Copy of Certificate

PQ 4	Company Presence	The company should be providing Data Center related services in India for at least the last 3 years (3) financial year ending 31st March 2019.	Self-Undertaking
PQ 5	Company Presence	The CSP should have multiple Data Centers facility in India.	Self-Undertaking
PQ 6	Company Presence	CSP should have a different seismic Zone across India/ MEITY compliant.	Self-Undertaking
PQ 7	Blacklisting	The Bidder should not be debarred/ blacklisted by any Government/PSU in India as on date of submission of the Bid.	A self-certified letter signed by the Authorized Signatory of the Bidder as per Annexure A.
PQ 8	Certification	Data Center and Disaster Recovery Center Facilities must be certified for ISO 27001 / 27018 (year 2013 or Above) and provide service assurance and effectiveness of Management compliant with ISO 20000 standards.	Valid Copy of the ISO 27001 / 27018, ISO 20000 Certification
PQ 9	Capability	CSP/MSP should have at least 5 operational Government Community Cloud client from Central/State/PSU departments during the time of bid submission. CSP has to submit the relevant document.	Work order + Completion Certificates from the client;
PQ 10	Capability	CSP/MSP must have experience of providing DC/DR hosting services in their data center at least 5 clients from any Central Govt/State Govt/Semi-Govt/PSU organization with a minimum order value of 10 Crores.	Work order + Completion Certificates from the client;

PQ 10	Network Connectivity	Proposed DR site should have feasibility for network connectivity of BSE, NSE, MCX & ICX	Self-Declaration by Managed & Cloud service provider on Letter Head with authorized signatory
PQ 11	Compliance	Service Provider (SP) should be empanelled with MeitY. Bidder shall provide documents of evaluation by MeITY / audit by STQC to the satisfaction.	Letter of Empanelment and STQC report

- Managed Service Provider and Cloud Service Provider may be single entity, in such cases will need qualify for conditions of Managed Service Provider and Cloud Service Provider.
- Managed Service Provider shall be solely liable to and responsible for all obligations towards the performance of works/services including that of its partners/associates under the contract.

3.22 Evaluation of Prequalification Proposals

1. Bidders, whose EMD and RFP Document Fees are found in order, shall be considered for Pre-Qualification criteria evaluation.
2. Bidder shall be evaluated as per prequalification criteria mentioned at Section 3.23. The bidders who fulfil all the prequalification criteria and technical demo shall qualify for further commercial evaluation.
3. The Bidders are required to submit all required documentation in support of the evaluation criteria specified (e.g. Detailed Project citations and completion certificates, client contact information for verification, and all others) as required for prequalification evaluation.
4. At any time during the Bid evaluation process, SSL may seek oral / written clarifications from the Bidders. SSL may seek inputs from their professional and technical experts in the evaluation process.
5. SSL reserves the right to do a reference check of the past experience stated by the Bidder. Any feedback received during the reference check shall be taken into account during the pre-qualification evaluation process.

3.23 Technical Evaluation Criteria

Criteria Evaluation Maximum Documents : Parameters Marked Required

TQ 1	Experience of Bidder in offering cloud services (IaaS) in India or Globally	1-3 years : 6 marks 4-6 years : 8 marks 7+ years :10 marks	10	Project Work order / Completion Certificates from the client stating Project Start date and Project End date
TQ 2	Tier Classification of the proposed Data Center, where cloud hosting is to be served from :	Tier III & Above: 10 marks	10	Valid Copy of the Tier III or Tier V Certification, certified under TIA 942 or Uptime Institute certifications by a 3rd party
TQ 3	Data Centre Uptime in Last 4 quarters	<99.5% : 2 marks 99.5-99.9% : 5 marks >99.9% : 15 marks	15	Self-undertaking
TQ 4	Number of VMs running (active) in the DC of the bidder	200-400 VM's : 6 marks 401-600 VM's : 10 marks >=601 VM's : 15 marks	15	Self-undertaking
TQ 5	Compliance to functional requirements	If compliance >95% - 15 marks 85-95% - 10 marks 70-85% 5 marks	15	Compliance sheet as per section 4.11.2 to be submitted, signed and stamped by Authorized Signatory
TQ 6	Project experience as per above eligibility requirement.	1 project : 3 marks Every additional project: 3 marks, max. upto 15	15	Project Work order and Completion Certificates

TO 7	Service Provider (SP) should be empanelled with MeitY.	Document	20	Letter of Empanelment and STQC report
Total			100	

TQ 7	Technical Presentation	Bidders understanding of the project and Scope of Work	300	
		Technical Solution		
		Project Management Methodology and People / Resources		
		System Architecture, Network Architecture and security		
		Clarifications / Answers given to the Bid Evaluation Committee during the Presentation -		
		Total	300	

POC	Marks
Service provider should deploy public facing services in a zone (DMZ) different from the application services. The Database nodes (RDBMS) should be in a separate zone with higher security layer.	
All access & changes carried out are logged, cannot be tampered with & be auditable.	
Workflow configuration for switch over from primary site to DR site.	
Dashboard to monitor RPO and RTO of each application and database.	
Performance the demo to access the service from DR site for certain users.	
Monitor the network traffic on servers.	
Monitor of network latency.	
Monitor network uptime of each device.	400
Monitor of resource utilization graph CPU, RAM, Disk and Network Bandwidth.	
Application performance monitoring.	
Database performance monitoring.	
Service Monitoring.	

3.24 Technical Evaluation Methodology

1. The Financial Proposals of Bidders who do not qualify technically shall be kept unopened.
2. SSL reserve the right to accept or reject any or all bids without giving any reasons thereof.
3. SSL shall inform to the technically shortlisted Bidders about the date and venue of the opening of the financial proposals.

Technical evaluation will be done based on the below calculations,

Bidder	Tech Marks Scored (A)	Out of (B)	Tech Marks (TM)= A/B*100	Tech. W'tage TW = 0.7	Tech. Marks TMW = TM x TW
CSP 1	700	900	77.78	0.7	54.44
CSP 2	750	900	83.33	0.7	58.33
CSP 3	680	900	75.56	0.7	52.89

3.27 Commercial Evaluation

1. Of all the financial proposal opened, the Bidder whose financial proposal is lowest (hereby referred to as L1 Bidder) shall be considered as most eligible for award of contract.
2. If there is a discrepancy between words and figures, the amount in words shall prevail. For any other calculation/ summation error etc. the bid may be rejected.

3. Grand total for the fixed components will carry a weight of 95%. (Denoted by X)
4. Price discovery elements (variable component) will carry a weight of 5%. (Denoted by Y)
5. The overall commercial score will be determined on basis of formula given below, following which the bidder with the highest score will be awarded the contract.
6. Z = 95 * X min / X + P1 * Y1 min / Y1 + P2 * Y2 min / Y2 + P3 * Y3 min / Y3
7. Where X is the grand total of the lump sum components for a specific bidder,
8. X min, is the least score amongst all the bidders for the lump sum components,
9. Y1 is the value of the price discovery element #1 (there are 3 such elements listed in table below) identified for increase in scope, (Similarly Y2, Y3, are values for element #2, element #3 respectively)
10. Y1 min, is the least quote amongst all the bidders for the price discovery element #1, (Similarly Y2min, Y3min are least quotes for element #2, element #3 respectively)
11. P1 are the points allocated to element #1 (Similarly P2, P3 are values for element #2, element #3 respectively)

For example if we have CSP 1, 2 and 3 quoting rates as given below:

#	Item	Points	CSP 1	CSP 2	CSP 3
P1	GCC Hosting for DR Site Infrastructure	2	4,00,00,000	3,00,00,000	3,00,00,000
P2	Managed Services for DR site	2	2,00,00,000	3,00,00,000	3,00,00,000
P3	Optional component in the rate card	2	1,00,00,000	2,00,00,000	3,00,00,000
Total Project Value for the 5 Yrs. Without Taxes			7,00,00,000	8,00,00,000	9,00,00,000

CSP	Grand Total (Fixed Components) (INR)	Score 1 (95 * X min / X)	Score 2 (P1 * Y1 min / Y1+ …. + P3 * Y3 min / Y3)	Fin. Score (Score 1 + Score 2)	Fin. W'tage FW= Total score x

					0.3
1	7,00,00,000	95.00	4.6	99.6	29.88
2	8,00,00,000	83.13	5.33	88.46	26.54
3	9,00,00,000	73.89	5.67	79.56	23.87

Example of calculations for CSP 2 are described as given below:

Score 1: 95 * 70000000.0 / 80000000.0 = 83.13 (The lowest bid for this component X min is Rs.7000000.0 from CSP 1, and CSP 3's quote is Rs.8000000.0)
Score 2: P1 * Y1 min / Y1 + P2 * Y2 min / Y2 + P3 * Y3 min / Y3
Score 2 : 2*500/500+ 2*1000/1000 + 2*1000/1000+ 1*80/120 = 5.33
The Fin. score for CSP 2: Score 1 + Score 2 = 88.46
The fin. Weightage for CSP 2 = 88.46 x 0.3 = 26.54

CSP	Tech. Marks TMW = TM x TW	Fin. W'tage FW= Total score x 0.3	Total TMW + FW
1	54.44	29.88	84.32
2	58.33	26.54	84.87
3	52.89	23.87	76.76

Based on the above matrix the contract will be awarded to CSP 2, as CSP 2 has the highest score of 84.87 marks

3.28 Award of Contract

3.28.1 SSL's Right to accept any Bid and to reject any or All Bids

SSL reserves the right to accept or reject any Bid, and to annul the bidding process and reject any or all Bids at any time prior to award of Contract, without thereby incurring any liability to the affected Bidder or Bidders or any obligation to inform the affected Bidder or Bidders of the grounds for SSL's action.

3.28.2 Letter of Acceptance

Prior to the expiration of the period of bid validity, SSL will notify the successful bidder in writing or by fax or email, to be confirmed in writing by letter, that its bid has been accepted. The Letter of Acceptance will constitute the formation of the contract. Upon the Successful Bidder's

furnishing of Performance Security Deposit, SSL will promptly notify each unsuccessful Bidder.

3.28.3 Signing of Contract

SSL shall notify the successful bidder that its bid has been accepted. The Successful Bidder shall enter into contract agreement with SSL within the time frame mentioned in the Letter of acceptance to be issued to the successful bidder by SSL.

3.28.4 Failure to agree with the Terms & Conditions of the RFP / Contract

Failure of the successful Bidder to agree with the Terms & Conditions of the RFP / Contract shall constitute sufficient grounds for the annulment of the award, in which event SSL may invite the next best bidder for negotiations or may call for fresh RFP.

3.29 Award Criteria

1. The bidder who has quoted the least will be adjudicated as most eligible for award of the Project.
2. However, SSL reserves the right to further negotiate the prices quoted by the most responsive bidder.

3.30 Non-Disclosure Agreement (NDA)

The Successful Bidder(s) has to sign the Non- Disclosure Agreement (Annexure C) with SSL.

2. Bid Prices

The vendor has to quote for "**Hiring of "Cloud based Disaster Recovery Services" from Managed Service Provider for SHCIL Services Ltd(SSL)"**, in the format given for financial bid. Validity of Bid shall be of 180 days from date of opening of bids.

3.31 Bid Currency

The rates quoted shall be in Indian Rupees only.

3.32 Signature

A representative of the bidder, who is authorized to commit the bidder to contractual obligations, must sign with the bidder's name and seal on all pages of the Bid, including the tender/bid document. All obligations committed by such signatories must be fulfilled.

3.33 Correction of errors

The vendor is advised to take adequate care in quoting the rate. No excuse for corrections in the quoted rate will be entertained afterwards. The corrections or overwriting in bid document should be initialed by person signing the Bid form.

3.34 Corrections to Arithmetic errors

In case of discrepancy between the amounts mentioned in figures and in words, the amount in words shall govern. The amount stated in the Bid form, adjusted in accordance with the above

procedure, shall be considered as binding.

3.35 Disqualification

The Bid from the bidders is liable to be disqualified in the following cases:

1. Bid not submitted in accordance with the bid document.
2. The bidder qualifies the bid with his own conditions.
3. During validity of the Bid, or its extended period, if any, the bidder increases his quoted prices.
4. Bid is received in incomplete form.
5. Bid is received after due date and time.
6. Bid is not accompanied by all requisite supporting documents.
7. Information submitted in Pre-Qualification Bid is found to be misrepresented, incorrect or false, accidentally, unwittingly or otherwise, at any time during the processing of the contract (no matter at what stage) or during the tenure of the contract including the extension period if any.
8. The successful bidder fails to enter into a contract within 10 working days of the date of notice of award of contract or within such extended period, as fixed by SSL.
9. Awardee of the contract has given the letter of acceptance of the contract with his conditions.
10. Non-fulfilling of any condition/term by bidder.
11. Submission of Bid without Tender Fees i.e. Rs.5000/- (Non Refundable)

4. Scope of Work

SSL wishes to engage a Managed Service Provider to provide Cloud based Disaster Recovery services for a period of 3 years post Go-Live for this project.

Scope of Work Overview

The scope of the project includes designing, implementing & maintenance of Government Community Cloud in

Data center (DC) for hosting applications as per the landscape for DC given. Bidders are also required to prepare project planning including VM specifications, installation, testing, implementation, plug-in add-on requirements, user training, looking ahead for five years.

The expected outcome from this project are the deployed on to Government Community Cloud in a third party Data Centre (DC).

The tasks associated with this project are broadly classified into five categories namely

1. Designing & Implementation
2. Project management
3. Provisioning of Government Community Cloud
4. DR setup on Cloud with replication between DC & DR
5. Post implementation support.
6. CSP must be a Meity empaneled for GCC Cloud Services & hosting services, along with the valid certificate.

Bidder needs to submit details like Architecture diagram, VM sizing, Security solution, Storage sizing with IOPs delivered, Project Plan, Approach & Methodology for deployment on Government Community Cloud on Data Center and Post implementation support methodology.

1.1 Designing & Implementation: -

As part of designing and implementation methodology, bidder needs to submit the details of

1. Provide technical solution design document of DR DC.
2. Compute must be sized at 50% during normal operations at primary site and during DR drill compute must be make 100%.
3. Perform all system software installations and updates for software considered under this RFP.
4. Proposed Solution should be compatible with IPv6 and High level architectural diagram showing different layers of solution like Internet / MPLS Connectivity, Network, Security, Compute, Hardware, Storage & Backup layers.
5. Proposed solution should have IP schema depicted at high level with nating to secure the applications directly getting exposed to Internet. Bidder should propose to deploy different applications and database in different VLANs with restricting users to directly access database layer and storage layer.
6. Backup solution with different features, like snapshots of VM's, online RDBMS backup, incremental and full back up of all data, restoration of data in test environment or as and when required.
7. Compliance sheet for the features mentioned in the following section for Cloud specifications.
8. Develop, maintain and update processing policies, procedures and documentation related to BCP.

1.2 Project Management: -

Selected service provider will be required to perform the following project management tasks for the assigned areas:

1. Provide a detailed work plan for different stages mentioned above.
2. Provide test plan for testing the new setup at new data center (IDC).
3. Provide BCP planning approach and methodology.
4. Provide training for the project team and assist in management of project progress.
5. Provide the complete technical documentations.
6. Successful bidder shall nominate a Project manager for entire period of the contract for interacting with <CLIENT> nominated person for the DR related activities.
7. Maintain project communications and provide documentation and adhere procedural standards approved by <CLIENT> for the execution of the project.
8. Prepare a service management plan for meeting the desired performance.

9. Planned backups should be maintained at the DR to recover from a crash / or any disaster.

1.3 Provisioning of Government Community Cloud: -

Cloud service provider to setup complete environment on Government Community Cloud to host ERP, service provider will be required to perform the following technical tasks for the assigned areas.

10. Setup Government Community Cloud with VM's designated for individual ERP modules.
11. Different VLAN's to be created to segregate front ending servers and database servers.
12. Storage proposed for DC should support IOPs as required.
13. VM's provisioned should have feature of vertical auto-scalability of resources like vCPU & RAM without requiring any manual intervention or to reboot the VM, in case there is sudden traffic on the server or if the number of users increase then the VM should detect the incoming traffic and accordingly should scale the resources.
14. Service provider should propose firewall, load balancer & security solution to protect the VM's, Application, Database from any type of external attacks like Virus attack, DDOS attack, hacking attempt, etc….
15. Detailed Cloud specifications and features are given in further section.

1.4 DR setup on gc Cloud with replication between DC & DR: -

Setting up of DR site on GCC. Service provider will be required to perform the following technical tasks for the assigned area:

1. Provision of GCC instance.
2. Provision and configuration of Network and security devices.
3. Provision of replication link.
4. The virtual cloud solution proposed should have auto-scalability to handle load during normal & peak period.
5. Setup replication between DC & DR.
6. Provide complete BCP planning report.
7. Approach on how service provider will meet the given RTO & RPO.
8. Propose replication monitoring tool to configure DR to be invoked with a single click. Other specifications of replication monitoring tool is given further.
9. Generate reports to ensure RTO & RPO are met as per the set timelines.
10. Provide technical solution design document of DR including DR switchover (Planned / Disaster) and switchback (Planned / Disaster) as per disaster recovery parameters given below:

a. Perform DR related activities including DR planning, testing, Drills, Switchback of DC in case of disaster recovery, etc.
b. Till a disaster (planned/ testing or otherwise) is declared by <CLIENT> the users should not be allowed to access the SAP application from DR site.
c. Provide Event Analysis Reports for the disaster recovery solution as a part of the services.
d. Provide a monitoring tool with dashboard showing RPO, RTO, changeover facility etc….
e. During the DR drill, the bidder need to arrange the full DR team with sufficient resources and expertise and complete the activity under the supervision of senior resource for co-ordination.
f. DR drills should be planned and executed periodically, minimum once in a quarter. Drills should be carried out over a minimum period of 24 hours each time. Drills can be conducted for all applications together which could simulate the failure of all systems.
g. The service parameters to be met by the DR system focus on the Recovery Time Objective (RTO) and the Recovery Point Objective (RPO), which define the interruption to service and loss of data respectively. RPO timeline is 30 minutes and RTO timeline is 1 hours.
h. The RTO will be calculated from the time of "declaration of a disaster" up to the time by which all the applications are made fully operational & end users are able to access these applications & carry out the business operations.
i. The exact process of the DR drill should be formulated in consultation with the <CLIENT> team in a way that all elements of the system are rigorously tested, while the risk of any failure during the drill is minimized. The process should be documented by the successful bidder as part of the disaster recovery plan.
j. The date, time, duration, and scope of each drill shall be decided mutually between <CLIENT> and the successful bidder. Extreme care must be taken while planning and executing DR drills to ensure that there is no avoidable service interruption, data loss, or system damage at DC.

1.5 Post Implementation Support: -

Post implementation support will be commenced in two parts, first for primary data center, after successful Go-Live of SAP ERP from Government Community Cloud. Following maintenance support is required to be provided by the shortlisted bidder at least for a period of five years.

1. Server, Storage, Networking Devices, Security Devices, Operating System, Backup administration and day to day management & troubleshooting in case of any problem.

2. Complete monitoring and maintenance of DC infrastructure, Cloud infrastructure, network, security, storage & backup, etc…
3. Maintenance of Configuration Changes in the already implemented Modules.
4. Application Support, monitoring and management will be taken care by application vendor.
5. Provide 24 x 7 x 365 days support for the entire solution including but not limited to proposed VPC, network, security and Backup solution proposed.
6. Propose helpdesk system to allow <CLIENT> users to call or log issues via phone or ticket.
7. Number of Phone calls, chats and ticket's should be unlimited.
8. At Disaster Recovery Site only production environment will be deployed along with the Solution Manager and Sap router.
9. The Bidder has to share the all User Name & Password with <CLIENT> authorized team.
10. ERP software will be provided by <CLIENT>. The infrastructure will be owned and managed by the bidder/ Service Provider. The proposed DC Site platform should be hosted in at least Tier 3 certified Data Centre and it should be located within the boundaries of India.
11. Any other technical support required in integrating existing network / security infrastructure of DC will also to be provided by the bidder.
12. A sufficient internet bandwidth should be provided for smooth access of applications with 99.95% cloud infrastructure uptime.
13. Manage IT Infrastructure implemented for <CLIENT> with 24 x 7 x 365 basis during the entire period of contract including help desk support.
14. Manage and maintain all Information security software, appliances and component.
15. Security Administration, virus protection and upgrades.
16. Service provider must ensure the security of services and data hosted at DC site.
17. Service provider shall transfer data back to <CLIENT> either on demand or in case of termination of contract for any reason.
18. The service provider shall provide necessary training to <client> personnel to monitor the various SLAs, monitor the dashboard in event of switchover/switchback at the time of disaster (planned/testing or otherwise).
19. Installation, configuration, maintenance and upkeep of 10 Mbps point to point Leased Line Connectivity with backup connectivity from Cloud Service Provider to SSL, inclusive of labor cost, consumables cost, civil work like digging, trenching, etc. and coordination with required authorities. Link shall be terminated at both SSL building (at distance of 300-500 meters) to ensure internet connectivity at all times. SSL may move its office to a new building (at distance of 100 meters) in future, service provider shall support, install and commission internet link. From DR site: Following exchange connectivity's should be there. BSE, NSE, MCX and ICX

4.1 General Requirements

Service Provider should ensure that the data should be residing within India. Data should only be accessed by entities authorized by SSL.

SSL shall retain ownership of any user created/loaded data and applications hosted on Service Provider's infrastructure and maintains the right to request (or should be able to retrieve) full copies of these at any time.

SSL retains ownership of all virtual machines, templates, clones, and scripts/applications created for the SSL's application. SSL retains the right to request (or should be able to retrieve) full copies of these virtual machines at any time.

Service Provider should be accessible via internet and P2P links

Service Provider should offer support 24 hours a day, 7 days a week, 365 days per year via its Network Operation Centre for monitoring and management of proposed IT infrastructure / Cloud services.

Service Provider should manage provisioned infrastructure as per the ITIL standards

Service Provider's shall provide interoperability support with regards to available APIs, data portability etc., for the Government Department to utilize in case of Change of cloud service provider, migration back to in-house infrastructure, burst to a different cloud service provider for a short duration or availing backup or DR services from a different service provider.

Shall adhere to the ever evolving guidelines as specified by CERT-In (http://www.cert-in.org.in/)

Shall adhere to the standards published (or to be published) by SSL or any standards body setup / recognized by Government of India and notified to the Service Provider by SSL as a mandatory standard.

The Service Provider's cloud service offerings will have to comply with the guidelines & standards as and when such guidelines / standards are published by SSL within the timeframe given by SSL. Service Provider is responsible for all costs associated with implementing, assessing, documenting and maintaining the empanelment.

Service Provider should offer monitoring tools that should monitor resources such as compute and other resources to gain system-wide visibility into resource utilization and operational health. SSL should get the appropriate visibility for the monitored information via a web dashboard.

It is expected that compute, storage, and bandwidth requirements may be auto-scaled (additional capacity based on the demand and auto-scaling rules) over the period of the contract in line with the transaction load to meet the SLA requirements. The application must be architected and designed to leverage the cloud characteristics such as rapid elasticity and handle transient and hardware failures without downtime.

The Service Provider will be responsible for adequately sizing the necessary compute, memory, and storage required, building the redundancy into the architecture (including storage) and load balancing to meet the service levels mentioned in the RFP.

It is expected that the Service Provider, based on the growth in the user load (peak and non-peak periods; year-on-year increase), will scale up or scale down the compute, memory, storage, and bandwidth requirements to support the scalability and performance requirements of the solution and meet the SLAs.

4.2 Infrastructure Analysis and Build

Under this phase Vendor needs to examine existing IT infrastructure and administrative functionality and applications at the primary data center of SSL (the "As Is" architecture) to make their Plan. During this phase a standard operating environment is created as a baseline "To Be" architecture.

Details of Existing Infrastructure: A. NSE Server

Sr. No.	Application Name	Server Type	Operating System	Database	Remark
1	NSE TAP Server	HP Proliant DL 360 G6	Windows 2008 Std Server 64 Bit	NIL	For NSE Segments Broadcast
2	NSE NEAT Adapter	HP Proliant DL 360 G6	Windows 2008 Std Server 64 Bit	NIL	For NEAT Terminals

B. ODIN Trading Application

Sr. No.	Application Name	Server Type	Operating System	Database	Remark
1	ODIN IML	HP Proliant DL 360 G6	Windows 2008 Std Server	NIL	For BSE Connectivity
2	ODIN Manager	HP Proliant DL 360 G8	Windows 2008 Std Server 64 Bit	NIL	Replication Required
3	ODIN Database	HP Proliant DL 360 G8	Windows 2008 Std Server 64 Bit	MS SQL 2005 64 Bit	Replication Required
4	ODIN SBS Server	HP Proliant DL 360 G6	Windows 2008 Std Server	NIL	One Time configuration
5	ODIN WEB Server	DELL MR630 Server	Windows 2008 Std Server	NIL	One Time configuration
6	IOB Server	DELL Poweredge R540 Server	Windows 2008 Std Server	Mongo Database	Replication Required

Concurrent Connection to ODIN Manager: 250
Concurrent Connection to ODIN WEB Server: 500

C. LD Back Office Application

Sr. No.	Application Name	Server Type	Operating System	Database	Remark
1	LD + LD CCM Database	HP Proliant DL 380 G8	Windows 2008 Ent Server 64 Bit	Oracle 11g	Replication Required

2	LD RAKSHAK + DIGI + IVR	HP Proliant DL 380 G8 Server	Windows 2008 Ent Server 64 Bit	Oracle 11g	Replication Required
3	LD WEB Server	DELL PowerEdge MR630 Server	Windows 2008 Ent Server 64 Bit	NA	One Time configuration
4	LD RAKSHAK Terminal	i-7 Processor Desktop	Windows 10 Professional	NA	One Time configuration

LD DB of Previous F.Y. + Current F.Y. = 500 GB
LD CCM DB = 500 GB plus
LD Rakshak = 500 GB
LD Digital= 1 TB (2 Financial Year Data)

No. of Concurrent Connections: LD 250

D: TRADEANYWHERE APPLICATION

Sr. No.	Application Name	Server Type	Operating System	Database	Remark
1	TAW WEB Server	DELL PowerEdge 630R Server	Windows 2008 Std Server	NA	One Time configuration
2	TAW TRADE Server	DELL PowerEdge 630R Server	Windows 2008 Std Server	NA	One Time configuration
3	TAW DATABASE	DELL PowerEdge 630R Server	Windows 2008 Std Server	MS SQL 2008 Std edition server	Replication Required
4	TAW Exchange Adapter	DELL PowerEdge 630R Server	Windows 2008 Std Server	NA	

Note: Above data usage is only approximate figure. Data usage is bound to change depending on user's requirement like uploading of documents, heavy files etc.

Software and Licensing Details: SSL is having below Licenses for Primary Data Center.

Sr. No	Description of Oracle	Metric	Term	Quantity
1.	Microsoft Windows 2008 Std. Server 64 Bit		Microsoft EA Agreement	
2	Microsoft Windows 2008 Ent. Server 64 Bit		Microsoft EA Agreement	
3	Microsoft Windows 2012 Std. Server 64 Bit		Microsoft EA Agreement	
4	Microsoft SQL Std. 2005 Server for ODIN		Microsoft EA Agreement	

B. Server Hardware Configuration

Sr. No.	Application Name	Core	RAM(GB)	HDD (RAID1)	Storage Connectivity(Yes / No) and Size	Operating System	DB / APP	Server Type
1	NSE TAP Server	4	8 GB	300 GB	No	Windows 2008 Std Server 64 Bit	APP	Physical
2	NSE NEAT ADAPTER Server	4	8 GB	300 GB	No	Windows 2008 Std Server 64 Bit	APP	Physical
3	IML Server	4	8 GB	600 GB	No	Windows 2008 Std Server	APP	Physical
4	ODIN Manager	16	32 GB	300 GB	No	Windows 2008 Std Server	APP	Physical
5.	ODIN DB	16	16 GB	300 GB	Yes (200 GB)	Windows 2008 Std Server	DB	Physical
6..	ODIN SBS Server	4	16 GB	300 GB	No	Windows 2008 Std Server	APP	Physical
7.	ODIN WEB Server	8	16 GB	600 GB	No	Windows 2008 Std Server	APP	Physical
8.	LD DB + CCM Database	8	256 GB	600 GB	Yes (1 TB)	Windows 2008 Ent Server	DB	Physical
9.	LD RAKSHAK + DIGI + IVR DB	8	128 GB	600 GB	Yes (1 TB)	Windows 2008 Ent	DB	Physical
10.	LD WEB SERVER	8	64 GB	600 GB	No	Windows 2008 Ent	APP	Physical
11.	LD RAKSHAK TERMINAL	4	16 GB	500 GB	No	Windows 2008 Std. Sever 64 Bit	APP	Physical
12	TAW WEB Server	4	16 GB	600 GB	No	Windows 2008 Std. Sever 64 Bit	APP	Physical
13	TAW Database Server	4	16 GB	600 GB	No	Windows 2008 Std. Sever 64 Bit	DB	Physical
14	TAW Trading Server	4	16 GB	600 GB	No	Windows 2008 Std. Sever 64 Bit	APP	Physical
15	TAW Exchange Adapter	4	16 GB	600 GB	No	Windows 2008 Std. Sever 64 Bit	APP	Physical

The current infrastructure mentioned above is provided for overall understanding of requirement at SSL. Bidder may visit SSL departments (On prior approval of SSL and its officials) and understand these requirements in detail.
The first step in this process is to identify the existing infrastructure applications. These applications include services that perform a business role and are required for proper functionality in DR environment. The analysis is conducted by working very closely with SSL's IT staff — reviewing installation methods, network topology, authentication procedures, and any existing documentation for third-party software. The bidder is expected to capture the current infrastructure details and SSL's requirements and propose optimal solution meeting SSL's requirement.

4.2.1 Infrastructure ecosystem mapping

Vendor should map SSL existing infrastructure applications to their Solution.

4.2.2 Operating System Build:

Bidder needs to study the existing infrastructure including operating system and provisioning of operating system at Cloud site should be planned accordingly.
Provisioning is composed of the following components:

- Provisioning configuration
  - Installation methodologies
  - Software packages (Third Party application will be done in coordination with the vendor)
  - Configurations according to security, authentication, storage, and other requirements
- Testing
  - Provisioning server setup
  - Deployment testing
  - Adherence to policy and configuration
- Delivery and training
  - Customer's IT staff trained to deploy and modify SOE build
  - Any remaining customer needs addressed
  - Additional training recommendations
- Documenting Results
  - Documentation
  - Detailing work performed
  - Specific procedures
  - Recommendations for future enhancements or growth
  - Links to product-specific manuals
- Fully tested provisioning server and provisioning configuration file(s)

- Time-tested and precise methodology, freeing up resources

4.3 Functional Application Analysis

4.3.1 Application Information Gathering

Vendor should examine existing documentation and conducting interviews with various IT and business stakeholders and should include below data in it:

- Existing hardware characteristics for different environments like production, staging, testing, and development environments
  - Number of hosts / CPUs per host
  - Memory requirements
  - Storage and file system requirements
  - Network bandwidth and latency requirements
  - Horizontal scalability requirements and/or limitations
  - Vertical scalability requirements and/or limitations
  - Hardware utilization rates
- Security requirements
- Authentication and authorization
- Versions and ISV support levels
- Specific software dependencies
- Development languages and platforms
- External integration points
- Virtualization restrictions
- Performance
- Stability

4.3.2 Third Party Application Porting Compatibility

The bidder should examine that application developed by third party software vendors are compatible to deploy on their platform. If there is anything which can't be port on their solution bidder should inform to SSL and SSL will coordinate with its ISV's in order to provide compatible code to their environment. Third party application developer (vendor) will be available for Pre-BID meeting.

4.3.3 Third Party Application Porting Dependency Mapping

The bidder should prepare a detailed mapping of application and its dependency. If any application has any dependency and involves any cost, bidder should inform same to the SSL.

4.4 Readiness and Risk Analysis

Since this is critical and larger environment, the bidder should study and submit a report of challenges endeavor from both an organizational readiness standpoint and a risk standpoint. Successfully identifying and mitigating both technical and organization risks is a

critical factor is important for DR Solution. The bidder and SSL both would require analyzing technical and organizational risks by using tools such as a SWOT (Strengths, Weaknesses, Opportunities, and Threats) analysis. Creating a comprehensive risk mitigation strategy outlining both preventative and compensatory actions will be necessary. Bidder shall carry out environmental feasibility study to identify environmental issues like corrosion etc at SSL DR Premises and shall implement appropriate solution to ensure smooth and zero- error performance of infrastructure.

4.5 Connectivity

The bandwidth connectivity of minimum 10 Mbps with backup link required for SSL to use the applications from the Cloud site and to ensure connectivity between SSL DC and proposed DR will be provided by the managed service provider as per the technical specifications. The managed service provider will be responsible for core infrastructure facility for provisioning of internet, point to point connectivity, including termination devices, network security in terms of Enterprise Class firewall and IPS/IDS.

4.6 Data Center Site at DR

- The service provider shall Configure and Monitor DR Site at Cloud Service Provider Premises and provide timely alerts for any issue via SMS, Email and Calls to contact persons of IT Department designated by SSL.
- Review and suggest modification in Disaster recovery plans and guidelines for SSL providing details of:
  - The key persons to be contacted during the disaster
  - The various activities to be done by vendor and SSL for complete operations from DR site and restoration of operations to main production site
- Service Provider shall provide standard operating procedures for smooth running and maintenance of Data Center site at DR for SSL.

4.7 Roles and Responsibilities of Service Provider

The service provider will be responsible for providing a tier 3 or above Cloud site within India.

- The Cloud site within India must be as per parameters mentioned in the Pre-Qualification criteria.
- Service Provider shall provide Single Point of Contact for all communication, resolution of issues and support required for smooth functioning of proposed cloud DR for SSL.
- The service provider shall develop, prepare and provide a Cloud Solution Implementation Plan. The Implementation Plan shall have the detailed design, specifications, drawings and schedule along with inspection and test plan, risk matrix and risk mitigation strategy, training material and documentation for all deliverables.
- Service Provider shall provide services comprising of, but not limited to, below items
  - Operating System Management
  - Network Management

- Security Management
- Storage Management
- Backup Management
- Disaster Recovery Management

- The service provider shall provision the cloud infrastructure, as and when ordered by SSL, as per scope of work defined in subsequent sections.
- The service provider responsible for the replication of data between the proposed DR site and Data Center of SSL. The service provider will be responsible for commissioning the bandwidth, as required by SSL, for replication of data and the SLA for the replication of data will be attributed to the service provider.

  The solution is envisaged for application level recovery scalable to site level recovery based on the impact of the disaster.

  SSL IT Team & the application vendor teams will support the Cloud Service provider during the deployment of the applications at the Cloud Solution site.

  Network setup (including switches, routers and firewalls) and uninterrupted network availability through a network link dedicated for connecting between the main DC site and DR site.

  Shared storage sizing for DR Cloud Hosting requirements.

  Necessary support in bringing the machines to login level in case of disaster / DR drills

  Provisioning, configuring and managing FC-IP router for DC to DR replication in case the proposed solution requires FC-IP router.

  Support during the recovery operations of data to and from DC-DR site.

  Ensuring related DNS changes for private WAN and internet, application availability and integrity, and database synchronization with application at DR site.

  24x7x365 support for Hardware restoration (from self and OEMs used), managed hosting support (including L1, L2, and L3 support), Uptime commitment up to OS levels, managed & monitored backup and backup retention (as per period required by SSL), OS provisioning & management, dedicated security services operations, etc.

  Monitoring and maintenance reports over a monthly basis and as and when required.

  Availability of server logs/ records for audits.

  Access to monitoring tools for measuring the service levels, application performance, server performance, storage performance and network performance.

  Support in audit of the entire system on a yearly basis.

  On expiration / termination of the contract, handover of complete data in the desired format to SSL which can be easily accessible and retrievable.

  Compliance process to the defined international standards and security guidelines such as ISO 27001, ISO 20000, ITIL, SEBI, Exchanges etc., for maintaining operations of cloud and ensuring privacy of SSL data. For the same an audit will have to be conducted on a periodic basis.

  The Cloud infrastructure and SSL data must be maintained ONLY at the location of the identified Cloud Hosting site. Data can only be moved to other site in case of any

emergency with prior approval of SSL concerned authority.

The bandwidth required for SSL to use the applications from the Cloud site will be provided by the service provider as per the technical specifications. The service provider will be responsible for core infrastructure facility for provisioning of internet, point to point connectivity, exchange connectivity, including termination devices, network security in terms of Enterprise Class firewall and IPS/IDS.

Scaling the server and storage infrastructure up or down based on the needs of SSL.

- In case of reverse replication, since the DR site would be acting as main site, all the necessary support to run the environment has to be provided by the service Provider.
- Reverse Replication is necessary and envisaged when the DR site is acting as the main site. The solution should ensure consistency of data in reverse replication till the operations are not being established at the Cloud site. The RPO would be applicable in reverse replication also. The entire data should be made available for restoration at Primary Data Centre.
- SSL shall have sole propriety rights for data stored in Cloud Environment at all times.
- It will be the Service Provider's responsibility to ensure that back up data is in a format that is restorable at Primary Site or DR Site.

- SSL auditors should allow to inspect DR site during the audit period.

4.8 Security Requirements

- Identity and Access Management (IAM) that allows controlling the level of access to the users to the Service Provider's infrastructure services. With IAM, each user can have unique security credentials, eliminating the need for shared passwords or keys and allowing the security best practices of role separation and least privilege.
- Secure Access - Customer access points, also called API endpoints, to allow secure HTTP access (HTTPS) so that the Agencies can establish secure communication sessions with Cloud services using Secure Sockets Layer (SSL)/Transport Layer Security (TLS).
- Virtual Private Cloud with Private Subnets and Built-in Firewalls to control how accessible the instances are by configuring built-in firewall rules
- Multi-Factor Authentication (MFA)
- Data Encryption - Client Side and / or Server Side Encryption as required
- Dedicated Network Connection using industry-standard 802.1q VLANs
- Centralized Key Management
- DDoS Protection
- Service Provider should offer Dedicated application layer (Layer-7) security & user control platform which should be able to identify & prevent known & unknown threats (in real time basis) covering the related in-scope applications running on the network. The proposed solution should therefore integrate the user's identity repository (across all entities) to enforce authorized access to the related in-scope applications. The

solution must be designed to ensure that the performance of the overall applications is not impacted due to the implementation of the security solutions and the management console should be same for this offering.

- The solution should offer application control, user based control, host profile, threat prevention, Anti-virus, file filtering, content filtering, QoS and scheduling capabilities in DR site.

The proposed solution must support on appliance Per policy SSL and SSH decryption for both inbound and outbound traffic.
Should support creation of C&C signatures based on IP, URL and DNS and content based AV signatures to block all the variants.
It should have capability to blocks malware and its variants based on content based signatures also for malwares.
The proposed solution should provide visibility into unknown threats, with the collective insight. It should correlate and gains intelligence from sandbox services, URL filter services, own research team, artifact-level statistical analysis and third-party feeds, including closed and open source intelligence.
The solution should have provision to extend beyond the network, so that no application or attached device should be trusted. Instead of monitoring for patterns or malicious behaviors, or white-listing applications, an advanced endpoint protection should persistently enforce the Zero Trust model on endpoints.
The proposed solution must be in the Leader's quadrant in Gartner Magic Quadrant of Enterprise Firewalls for the last 3 years- 2018, 2017 and 2016.
The solution should be capable to identify and prevent in-progress phishing attacks by controlling sites to which users can submit organization credentials based on the site's URL category thus blocking users from submitting credentials to un-trusted sites while allowing users to continue to submit credentials to organization and sanctioned sites.
The proposed solution shall provide sandbox behavior based inspection and protection of unknown viruses and zero-day malware for any application and protocol (not limited to HTTP, SMTP, FTP) and the solution shall be able to provide automated signature generation for discovered zero-day malware and the solution should ensure the delivery of the signature in 5 mins from the time of detection. The analysis has to be done on premise and data should not go to cloud for analysis.
The lateral traffic between the virtual machines should get the same type of security as for north south traffic using virtual next generation security platform.
Service Provider should offer dedicated appliance based DDOS solution (not integrated on firewall and any other network device) with multi-tenant support for department vide policy enforcement and monitoring
Solution should detect and mitigate application layer DDOS protection for HTTP GET flooding, HTTP post flooding, HTTPS flooding, DNS flooding, DNS amplification, NTP amplification and other IP and TCP based attacks. support netflow v5, netflow v9, sflow v4, sflow v5, netstream v5, ipfix with out-of-line and inline deployment

Security Incident and Event Management (SIEM) tool offered in SaaS based model, which correlates the event logs and alerts from multiple network devices and servers in near real time

End point Antivirus and Antimalware, zero day protection for all mission critical servers / Virtual Machines

Solution should provide security service for the intelligence, analytics, and context required to understand which attacks require immediate response, as well as the ability to make indicators actionable and prevent future attacks. It should be capable of integrate with Third-party open-source application that streamlines the aggregation, enforcement and sharing of threat intelligence

Solution should have capabilities to analyze and correlating threat intelligence. For identified high-priority attacks, solution should enable organization to find related indicators of compromise (IOCs) and export them from the service so that organization can take immediate and decisive action to prevent threats and mitigate potential impact. It should allow IOC to be exported to external data which can be automatically integrated with enforcing points like Next gen firewalls.

Vulnerability testing on a half yearly basis. Reporting of the same on a half yearly basis

Secure access to SSL's infrastructure by Service Provider's authorized administrators via Privilege Infrastructure Management solution, that offer Identity, Authentication and Role based access to customer's Infrastructure

The MSP shall procure and implement the following security solutions provided by third party:

• Anti-Virus for the virtual machines •

Host Intrusion Detection System

• Web Application Firewall to help protect web applications from common web attacks such as SQL injection or cross-site scripting

• SIEM to monitor the security incidents

4.9 Audit and Governance Requirements

The Service Provider shall implement the audit & compliance features to enable the Agency to monitor the provisioned resources, performance, resource utilization, and security compliance.

- 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.
- Event-based alerts, to provide proactive notifications of scheduled activities, such as any changes to the infrastructure powering the cloud resources.
- 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.
- Review of auto-scaling rules and limits.
- 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.

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

4.10 Implementation Plan

The bidder should prepare and submit a detailed plan during execution of order with following details:

4.10.1 Consolidated Analysis of existing hardware:

Mapping of detailed hardware at DR site should be prepared with detailed analysis including following parameters:

- CPU calculations
- RAM calculations
- Disk calculations
- Network interfaces requirement
- Network throughput requirement
- Backup requirement

4.10.2 Virtual Cloud Deployment

The solution should be deployed to offer minimum RPO and RTO. (Pilot-Light for Quick Recovery, Warm Standby for further reduced recovery time, and Multi-Site Solution Deployment for active-active deployment as per the requirements of the project and the design of the application being migrated to cloud.)

Detailed planning of Virtual Private Cloud deployment and configuration should be submitted to SSL. The configuration planning should include following details.

- Network architecture planning
- Firewall configuration planning.
- VLAN configuration planning

- IP address planning
- Subnet planning and routing planning
- Backup methodology
- Failover mechanism for replication links

4.10.3 System Planning:

Once the architecture is ready to be provisioned on Cloud, the bidder should prepare detailed plan of system planning. This planning would require following details.

- On line and full off line backup of existing system.
- Notification of downtime to end users.
- System export window
- Replication tool configuration
- Transfer time of data from DC to DR
- Data restoration at DR side.
- Data Sync times and dependencies if any
- Switching on DR servers
- Notifying end users.
- Coordination with other vendors (Application Vendors /SSL IT Team)

Detailed planning of Disaster Recovery deployment and configuration should be submitted to SSL. The configuration planning should include following details.

• Network architecture planning including
    - VLAN configuration planning
    - IP address planning
    - Subnet planning and routing planning
- Firewall configuration planning
- Backup methodology
- Failover mechanism for replication links
- Business continuity Architecture planning

On acceptance of the Implementation Plan by SSL, the service provider shall implement the cloud solution and offer for testing.

4.10.4 Testing Planning

Following cloud resource deployment/provisioning, the testing of the same at Cloud site becomes very important. Therefore the service provider must perform following testing:

4.10.4.1 Functional Testing

Once system is exported, data is migrated to Cloud site and application started functioning,

the functional testing of Application will be done by SSL Team along with application vendors. The bidder requires to provide support and co-ordination in this case. SSL and application vendors may perform following testing.

- Software Module testing as per functional requirement.
- User authentications testing.
- Users add/delete, reports generations
- Heavy application transactions on DR servers.
- Backup exports
- Backup restoration

4.10.4.2 Data Integrity Testing

Data integrations will be very important factor in overall process. Since data will be replicated over same or cross platform including same database at both end, the data integrity testing would become crucial. Data integrity testing will include:

- Amount of data verification at both end.
- Table size and records testing.
- Users status at both end.
- Invoices/transactions verification at both ends.
- Data in log files.

4.10.4.3 Business Continuity testing

To demonstrate how the application fails over when the primary site goes down. The testing should include the:

- Uninterrupted replication to DR servers.
- Lag in replication due to any unforeseen errors.
- Process of recovering from lags if any.
- Data integrity test of DR servers.

4.10.5 Service Maintenance

The bidder requires to maintain the resources provisioned on Cloud. On Day to day basis bidder should send the reports of:

- Network monitoring
- Security monitoring and analysis

If any application patch has to be applied, it will be applied by SSL and its software application vendors.

4.10.6 Failover

In the event of a disaster, the system at Proposed Bidder's DR Data Center will be primary system. All users of Company will connect to Bidder's system through Internet link. Since the systems has been asked on virtual private cloud infrastructure, all systems should be auto

scalable. Whenever load of users will grow, the systems should scale resources automatically in terms of RAM and CPU. The failover from Main DC to DR should be done through a proper DR announcement process which should be documented as part of BCP planning.

4.10.7 Restoration

Restoration provides an easy process for copying updated data from the DR server back to the DC server. Whenever main DC will be recovered and operational, the data from DR system to DC systems should be synchronized. Once this data is synchronized and verified, the switchover from DR system to DC system should be done. In that case all users will be accessing systems of main DC.

4.10.8 Implementation of Project

The Bidder's proposal shall specify the project management methodology which would be used for this infrastructure setup and ensure compliance to relevant standards so as to make this equivalent to a Tier III data center.

The responsibilities of the bidder during this project over its logical broad phases are outlined in the subsequent sub-sections. The ongoing responsibilities of bidder during the project are also outlined below.

The activities / deliverables mentioned below are not exhaustive. The Bidder is expected to complete all activities / provide deliverables required to build the infrastructure in line with the quality / service standards prevalent in the industry for such infrastructure

4.10.8.1 Phase 1: Project Preparation

During the first phase of project, the Bidder should prepare the project charter. The Bidder should also provide assistance in outlining the solution deployment architecture with details of hardware and Operating system platform and disaster recovery architecture. Some of the important activities / deliverables during this phase would be

1. Project Management Plan

The Bidder should prepare the project management plan, which outlines the project objectives, timelines, project procedures and project organization and submit it to SSL for approval.

The Project Management Plan should include at least the following:

- Detailed methodology for setting up the DR infrastructure, dependencies etc.
- Risk Management Plan
- Quality Management Plan
- Escalation Procedures
- Approval Procedures
- Training Strategy and Plan

- Performance / Final Acceptance Test Plan for all components of the DR Solution.

2. Training Strategy

SSL believes that key to successful implementation will be the Bidder's ability to train SSL's staff in the operation of the proposed infrastructure:
As a part of the training strategy the Bidder should provide the following information:

- The facilities, support materials and program including mode of training (standard/ self-paced) provided for training the users in using the system.
- List of training areas for training to be provided to SSL identified personnel and technical team.
- Training infrastructure required and expectations from SSL , if any
- Duration and frequency of training

The training strategy should be designed to provide training to the IT technical team personnel identified by SSL at SSL site. SSL will measure the effectiveness after the completion of the training through training feedback forms. A formal training plan with relevant course material is required as part of the training session.

3. Project Plan

The Bidder shall develop a detailed Project Plan. The Project Plan shall amongst other functions, detail all tasks including but not limited to the task / person in charge for the execution of the task/ effort resource allocation. This information shall be provided in the form of a detailed Gantt chart. The Project Plan shall also detail all milestones and indicate when the required deliverable / documentation will be available to SSL. This plan will be discussed with SSL and finalized during the project preparation stage.

4.10.8.2 Phase 2: Provisioning of Cloud Setup

The Bidder's team should study the existing infrastructure of SSL and the requirements of the solution and build the Cloud infrastructure accordingly. DR Cloud Infrastructure readiness is the sole responsibility of the successful bidder. Interfaces with various agencies required to carry this out is the responsibility of the bidder.
Some of the important activities / deliverables during this phase would be:

- DR Site should confirm to Tier III Standards or above.
- Provisioning the resources on Cloud
- DR Data Center should be in India

4.10.8.3 Phase 3: Commissioning, Testing and Training

During this phase of project, the Bidder will establish and commission the systems as per the specifications. The Bidder team will carry out the required customization / clustering /

virtualization of servers to meet the requirements. Bidder should pass the configured system through its own internal quality processes and provide the compliance reports to the SSL team. Training will also form part of this phase.

4.10.8.4 Phase 4: Post Go Live Support

Bidder should provide post- Go Live support & DR Services support for entire contract period of three years as applicable. The support should be provided through help-desk support mechanism as defined below. It is assumed that the entire system would be stabilized at the end of post Go Live support.

4.10.8.5 Help Desk Support

Bidder is required to create and maintain a Help Desk / telephonic number that will resolve problems and answer queries related to disaster recovery site and its equipment supplied by the bidder.

The help desk support to users shall be provided on 24x7x365 basis over telephone, chat and ticketing system. The details regarding telephonic, chat & ticketing support will be carefully considered, as this will have effect on the support response to SSL system end-users. The Bidders response and resolution time will be the basis for end- user support time in SSL"s service level agreements with the Bidder.

4.10.9 Documentation

This documentation should be submitted as the project undergoes various stages of implementation. Indicative list of documents include:

- Detailed Project Plan
- Project Management Plan

- Training Material should be provided which shall include the presentations used for trainings and also the required relevant documents for the topics being covered.

The selected bidder shall document all the installation and commissioning procedures and provide the same to SSL within one week of the commissioning of the DR Site. The selected bidder shall be responsible for documenting configuration of all devices / equipment and keeping back up of all configuration files, so as to enable quick recovery in case of failure of devices.

4.11 Project Timelines and Payment Terms

T= Issuance of LOA

Sr.	Milestone	Deliverables	Timelines	Payment Terms *
1	Acceptance of LoI/Work Order/Contract (whichever is earlier)	**Signed Contract**	Project Start Date (T)*	Nil
2	Project Implementation Plan	Project kick off meeting, Project Inception Report covering approach & Project Plan	T + 2 Weeks	Nil
A) Design , Configuration, Testing, Installation and Setup				
3	Network /Communication Links	Design , Configuration, Testing, Installation and Setup of ILL, Exchange Connectivity	T+ 2 month	100% of Network
4	Cloud Solution Implementation and Migration	Provisioning of the cloud resources and Migration of the application on new Cloud Environment	T + 1 months	Nil
5	Operational Acceptance and Go- Live	User Acceptance Test Report, Operational Acceptance Report, Go-Live report	T+ 45 days	Nil
B) C	**oud Operation and Management (During O&M Period)**			
6	Cloud Service Components offered	Cloud Resources Provisioning and Various MIS and Helpdesk Reports as described in this tender	As Required by SSL	Quarterly payments (QP) at end of quarter, on usage basis, after deducting all applicable penalties

- No Advance payment against Purchase Order or Work order.
- All payment shall be released after submission of bills for quarterly period.
- Payment shall be made only for actual services, components utilized on hourly, monthly basis during quarter by SSL.

4.11.1 Contract Period

The contract will start as per the date of award of the work order and will be valid for 3 years post Go-Live. The rates quoted will be valid for contract duration.

4.11.2 Specifications and Requirements

4.11.2.1 DR Data Center Facility Requirement

SSL seeks a DR data center facility that meets the following requirements. The requirements set forth below are intended to serve as a baseline reference only. Offers shall submit detailed descriptions of their data center facility.

- **Data Centre** : Cloud Services must be offered from a Data Center that is conforming to Tier III standards or above. Data Center should be in India
- **Cloud Hosting**: SSL looking for a stable, scalable and secured cloud infrastructure. In case, in future SSL want same cloud infrastructure should be used as a production site. So proposed cloud platform should be horizontal and vertical scalable.
- **Connectivity** : Cloud DR Data Center should have feasibility of BSE, NSE & MCX exchanges connectivity.
- **Reporting**: CSP should provide several reports wrt utilization and performance.
- **Availability**: uptime / availability of compute (99.5%) and Storage (99.5%)
- **Industry Standards**: SSL seeks a data center complaint with industry standards as defined by (but not limited to) ISO 27001 / ISO 27018
- **RTO** <= 1 hours
- **RPO** <= 30 mins

Support

	Requirement	Description	Compliance (Y/N)	Remarks

1	Service Health Dashboard	Cloud provider should offer a dashboard that displays up-to-the-minute information on service availability across multiple regions.		
2	365 day service health dashboard and SLA history	Cloud provider should offer 365 days' worth of Service Health Dashboard (SHD) history.		
3	Monitoring Tools	Monitoring tools that will enable collection and tracking metrics, collection and monitoring log files, set alarms, and automatically react to changes in the provisioned resources. The monitoring tools should be able to monitor resources such as compute and other resources to gain system-wide visibility into resource utilization, application performance, and operational health.		

4.12 Commissioning

Commissioning of the System (or Subsystem if specified in the Contract) shall be commenced by the service provider:

- Immediately after the Go-Live Certificate is issued by SSL.
- as otherwise specified in the Technical Requirement or the Agreed and Finalized Project Plan;

4.13 Operational Acceptance

- Operational Acceptance shall commence on the system, once the system is commissioned to a period of maximum 30 days.
- Operational Acceptance will only be provided after cloud resources and provisioned and switchover testing (as applicable) has been completed. Switchover testing would include:
  - Switch over of application from DC to DR as per defined RTO and RPO
  - Switch over applications from DR to DC as predefined RTO and RPO
  - Complete Data Replication and Reverse Data Replication as per RPO
  - Fully functional application while DR site is operational as confirmed by SSLL end users of application
- The service provider will have to facilitate the operational acceptance tests. Operational acceptance tests will be performed by SSL; however Service provider will have to facilitate operation acceptance during commissioning of the system (or subsystem[s]), to ascertain whether the system (or major component or Subsystem[s]) conforms to the scope of work, including, but not restricted to, the functional requirements. The service provider will have to facilitate the testing of all applications from SSLL users during the operational acceptance.
- After the Operational Acceptance has occurred, the Service provider may give a notice to SSL's Project Manager requesting the issue of an Operational Acceptance Certificate.
- Once deficiencies have been addressed, the service provider shall notify SSLL, and SSLL, with the full cooperation of the service provider, shall use all reasonable endeavors to promptly carry out retesting of the System or Subsystem. Upon the successful conclusion of the Operational Acceptance Tests, the Service provider shall notify SSLL of its request for Operational Acceptance Certification, SSLL shall then issue to the service provider the Operational Acceptance Certification, or shall notify the Service provider of further deficiencies, or other reasons for the failure of the Operational Acceptance Test. The procedure set out in this clause shall be repeated, as necessary, until an Operational Acceptance Certificate is issued.
- If the System or Subsystem fails to pass the Operational Acceptance Test(s), then either:
  - SSL may consider terminating the Contract, or
  - If the failure to achieve Operational Acceptance within the specified time period is a result of the failure of SSL to fulfill its obligations under the Contract, then the

    Service provider shall be deemed to have fulfilled its obligations with respect to the relevant technical and functional aspects of the Contract.

• Operational Acceptance will have to be performed for each phase.

4.14 Post Implementation Maintenance & Support

The service provider shall maintain and manage the system (cloud solution) for the entire period of the contract and shall be fully responsible for ensuring adequate CPU processing power, memory, storage, network, internet bandwidth and monitoring of the cloud services for optimum performance of the entire Cloud solution conforming to SLAs as per the Contract. The successful bidder has to provide post implementation support to maintain SLAs.

During the support period, if the successful bidder is unable to comply with the support terms, the bidder will have to a pay a Penalty as specified under the SLA of this project. Post implementation support would also include support during scheduled DR drills (once every 3 months), during regular operations while only replication is taking place, in disaster scenario when DR is active and operational, and during switchover and switchback.

4.15 Backup and Restore Services for DR

The Service Provider shall provide backup solution (LTO6 tapes, or Disk-based backup in conjunction with Tape based backup), policies and procedures that is suitable to SSL environment, in consultation with IT Department SSL. The activities shall include, but not limited to:

- Backup of operating system, Virtual Machines and application as per stipulated policies at the SSL.
- The Lifecycle of Backup will be 30 days
- Monitoring and enhancement of the performance of scheduled backups, schedule regular testing of backups and ensure adherence to related retention policies.
- Real-time monitoring, log maintenance and reporting of backup status on a regular basis. Prompt problem resolution in case of failures in the backup processes
  SSL will review backup and restoration mechanism from time to time, in line with advancement in the technologies and the backup/restoration mechanism would be finalized in consultation with the service provider. This will have no commercial bearings.

4.16 MIS Reports

Service Provider shall submit the reports on a regular basis in a mutually decided format. The Service Provider shall workout the formats for the MIS reports and get these approved by the SSLL within a month of being awarded the contract. The following is only an indicative list of MIS reports that may be submitted to the SSLL:

- Daily reports
  - Summary of issues / complaints logged at the Help Desk
  - Summary of resolved, unresolved and escalated issues / complaints
  - Summary of resolved, unresolved and escalated issues / complaints to vendors.

- Log of backup and restoration undertaken.

- Weekly Reports
  - Summary of systems rebooted.
  - Summary of issues / complaints logged with the OEMs.
  - Summary of changes undertaken in the Data Centre including major changes like configuration changes, patch upgrades, etc. and minor changes like log truncation, volume expansion, user
  - Creation, user password reset, etc.
  - Hypervisor patch update status of all servers including the Virtual Machines running on in
- Monthly reports
  - Component wise server as well as Virtual machines availability and
  - resource utilization
  - Consolidated SLA / (non)- conformance report.
  - Summary of component wise uptime.
  - Log of preventive / scheduled maintenance undertaken
  - Log of break-fix maintenance undertaken
  - All relevant reports required for calculation of SLAs
- Quarterly Reports
  - Consolidated component-wise availability and resource utilization.
  - All relevant reports required for calculation of SLAs
  - The MIS reports shall be in-line with the SLAs and the same shall be scrutinized by the SSL.
- The service provider will also provide any other report requested by the SSLL or any other agency approved and authorized by SSLL.

4.17 Input to Periodic Disaster Recovery Plan Update

The service provider shall be responsible providing input for

- Devising and documenting the DR policy discussed and approved by SSL.
- Providing data storage mechanism with from the Go-Live date till the date of contract expiry for the purpose of compliance and audit.

4.18 Hardware Upgrades & Software Updates

Any required version/Software /Hardware/ License upgrades, patch management etc. at the Cloud Site will be supported by the solution provider for the entire contract period at no extra cost to SSL. Application Patch updation will be done in coordination of Application Vendor and SSL IT Team.

4.19 Coordination, Cooperation and Support to FMS vendor of SSL

- During all phases of the project, the Implementation Agency shall have coordination and full cooperation with the FMS service provider / Application Technical support of SSL / SSLIT Team,. Since the project infrastructure has to be fully integrated with the SSLL IT Environment, the Implementation agency will require support and from FMS / Application vendor and vice versa.
- SSL shall ensure that FMS service provider shall cooperate with the implementation agency and provide all necessary support, configuration settings, access to requisite and necessary IT assets.
- The service provider shall support the FMS team / Application Vendor of SSL for the following activities:
  - Co-coordinating issues for timely resolution.
  - Knowledge Transfer of all activities performed by the service provider as part of installation, configuration, setup, operate and maintain.

4.20 Provisioning Cloud services for additional quantities at same rate

- Based on future requirements, SSL is likely to purchase additional quantities of cloud service covered in this Tender requirement.
- The rates offered cloud services must be valid for entire contract/project duration. No variation in these quoted rates shall be allowed during this period.
- SSL will have liberty to order additional cloud service items, at the rates offered in the commercial bid.

4.21 Service Level Agreement (SLAs)

- Cloud "Service Level Objective" (SLO) means the target for a given attribute of a cloud service that can be expressed quantitatively or qualitatively.
- Cloud SLAs means documented agreement between the service provider and the Department that identifies services and cloud service level objectives (SLOs).
- Response time is the time interval between a cloud service customer initiated event (e.g., logging of the request) and a cloud service provider initiated event in response to that stimulus.
- "Scheduled Maintenance Time" shall mean the time that the System is not in service due to a scheduled activity. Scheduled maintenance time is planned downtime with the prior permission of the Department, during non-business hours. The Scheduled Maintenance time <<within 10 hours a month>> as agreed shall not be considered for SLA Calculation.
- "Scheduled operation time" means the scheduled operating hours of the System for the month. All scheduled maintenance time on the system would be deducted from the total operation time for the month to give the scheduled operation time.

- "Availability" means the time for which the cloud services and facilities are available for conducting operations on the Department system.
- Availability is defined as:
- {(Scheduled Operation Time - System Downtime) / (Scheduled Operation Time)} * 100%
- "Incident" refers to any event/issue that affects the normal functioning of the services / infrastructure, reported by the cloud consumer to the Cloud Service provider (CSP) can be termed as an Incident.
- "Incident" refers to any event / abnormalities in the functioning of the IT Infrastructure solution and services that may lead to disruption in normal operations.
    i. "Helpdesk Support" shall mean the 24x7x365 centre which shall handle Fault reporting, Trouble Ticketing and related enquiries during this contract.
    ii. "Response Time" shall mean the time incident is reported to the help desk and an engineer is assigned for the call.
- "Resolution Time" shall mean the time taken (after the incident has been reported at the helpdesk), in resolving (diagnosing, troubleshooting and fixing) or escalating (to the second level) getting the confirmatory details about the same from the Agency and conveying the same to the end user), the services related troubles during the first level escalation.
- The resolution time shall vary based on the severity of the incident reported at the help desk. The severity would be as follows:
    - Critical : Critical/Central IT Infrastructure solution down impacting critical business functions or multiple modules/functions down impacting users on daily operations or any module/functionality deemed as highly critical by SSL .
    - High: IT Infrastructure solution down impacting critical business functions or multiple modules/functions down impacting users on daily operations or any module /functionality deemed as highly critical by SSL.
    - Medium: One module/functionality down impacting critical business functions having major impact on daily operations.
    - Low: Loss of business functionality for less than 10 users impacting day to day operations or minor functionality down impacting less than 10 users.
- Commencement of SLA: The SLA shall commence from implementation period itself for adherence to the implementation plan. The penalty will be deducted from the payment milestone during the implementation period. During the O & M period, the penalty will be deducted from the quarterly payments.

SLA Review Process and Penalty

a. Either SSL or bidder may raise an issue by documenting the business or technical problem, which presents a reasonably objective summary of both points of view and identifies specific points of disagreement with possible solutions.

b. A meeting or conference call will be conducted to resolve the issue in a timely manner. The documented issues will be distributed to the participants at least 24 hours prior to the discussion if the issue is not an emergency requiring immediate attention.
c. The SSL and the bidder shall develop an interim solution, if required, and subsequently the permanent solution for the problem at hand. The bidder will then communicate the resolution to all interested parties.
d. In case the issue is still unresolved, the arbitration procedures described in the Terms & Conditions section will be applicable.
e. Three consecutive quarterly deductions of more than 10% of the applicable fee on account of any reasons will be deemed to be an event of default and likely termination.
f. If the penalty reaches 10% of the total contract value, SSL may invoke termination clause.

For the Departments to ensure that the Cloud Service Providers adhere to the Service Level Agreements, this section describes the Penalties which may be imposed on CSPs. In case these service levels cannot be achieved at service levels defined in the agreement, the departments shall invoke the performance related penalties. Payments to the Service Provider to be linked to the compliance with the SLA metrics laid down below. To illustrate calculation of penalties, an indicative example is provided below.

a. The penalty in percentage of the <<Periodic Payment>> is indicated against each SLA parameter in the table.
    i. For ex: For SLA1 if the penalty to be levied is 7% then 7% of the <<Periodic Payment >>) is deducted from the total of the <<periodic> bill and the balance paid to the SP.
    ii. If the penalties are to be levied in more than one SLA then the total applicable penalties are calculated and deducted from the total of the <<periodic> bill and the balance paid to the SP.
    For ex: SLA1 =7% of the <<Periodic Payment>>, SLA12=10% of the <<Periodic Payment >>, SLA19=2% of the <<Periodic Payment>> then,
    Amount to be paid = Total <<periodic > bill - {(19% of the <<Periodic Payment>>)}

Periodic Payment - Quarterly Payment

T- Issuance of LOA

#	Service Level Objective Service Levels for CSP	Measurement Methodology /	Target/Service Level	Penalty
Implementation related SLAs				
1.	Network / Communication Links Design, Configuration, Testing, Installation and Setup of ILL Connectivity as required.	Within 2 month from the issuance of LOA (T) For Exchange connectivity 60 days	This will be calculated on basis of days of delay	a) Within 2 month from T - Nil b) For every 7 days of delay 10% of QP. The Bidder would be required to provide proper justification for the delay. If SSL feels that the justification provided by the Bidder is not credible, the contract may be terminated. Penalty shall be paid in Demand Draft payable to SHCIL Services Limited. Failure to pay penalty may result in penalty amount deducted

#	Service Level Objective	Measurement Methodology /	Target/Service Level	Penalty
				from Quarterly Payment
2.	Cloud Solution Implementation and Migration Provisioning of the cloud resources and Migration of the application on new Cloud Environment	Within one months	This will be calculated on basis of days of delay	a) Within one months from T - Nil b) For every 7 days of delay 10% of QP. The Bidder would be required to provide proper justification for the delay. If SSL feels that the justification provided by the Bidder is not credible, the contract may be terminated. Penalty shall paid in Demand Draft payable to SSL. Failure to pay penalty may result in penalty amount deducted from Quarterly payment.
3.	Operational Acceptance and Go-Live User Acceptance Test Report, Operational Acceptance Report, Go-Live report	Within 45 days	This will be calculated on basis of days of delay	a) Within 45 days from T- Nil b) For every 7 days of delay 10% of QP. If the Bidder fails to pass the operational acceptance even after 3 unsuccessful attempts, SSL

#	Service Level Objective	Measurement Methodology /	Target/Service Level	Penalty
				may consider terminating the contract. Penalty shall paid in Demand Draft payable to SHCIL Services Limited. Failure to pay penalty may result in penalty amount deducted from Quarter Payment.
Availability/Uptime				
1.	Availability/Uptime of cloud services Resources for Production environment (VMs, Storage, OS, VLB, Security Components)	Availability (as per the definition in the SLA) will be measured for each of the underlying components (e.g., VM, Storage, OS, VLB, Security Components) provisioned in the cloud. Measured with the help of SLA reports provided by CSP.	Availability for each of the provisioned resources: >=99.5% Monitoring shall be on monthly basis.	Default on any one or more of the provisioned resource will attract penalty as indicated below. <99.5% & >=99% (10% of the <<Periodic Payment>>) < 99% (30% of the << Periodic Payment>>)
2.	Availability of Critical Services (e.g., Register Support Request or Incident; Provisioning / De-Provisioning; User Activation / De-Activation; User Profile Management; Access Utilization Monitoring Reports) over User / Admin Portal and APIs (where applicable)	Availability (as per the definition in the SLA) will be measured for each of the critical services over both the User / Admin Portal and APIs (where applicable)	Availability for each of the critical services over both the User / Admin Portal and APIs (where applicable) >= 99.5%. Monitoring shall be on monthly basis.	Default on any one or more of the services on either of the portal or APIs will attract penalty as indicated below. <99.5% and >= 99% (10% of the <<Periodic Payment>>) <99% (20% of the <<Periodic Payment>>)

#	Service Level Objective	Measurement Methodology /	Target/Service Level	Penalty
3.	Availability of the network links at DR (links at DRC, DC-DRC link)	Availability (as per the definition in the SLA) will be measured for each of the network links provisioned in the cloud.	Availability for each of the network links: >= 99.5%. Monitoring shall be on monthly basis.	Default on any one or more of the provisioned network links will attract penalty as indicated below. <99.5% & >=99% (10% of the <<Periodic Payment>>) < 99% (30% of the <<Periodic Payment>>)
4.	Availability of Regular Reports		15 working days from the end of the quarter. If STQC issues a certificate based on the audit then this SLA is not required.	5% of <<periodic Payment>>
Su	**support Channels - Incident and Helpdesk**			
1.	Response Time	Average Time taken to acknowledge and respond, once a ticket/incident is logged through one of the agreed channels. This is calculated for all tickets/incidents reported within the reporting month.	95% within 15 minutes	<95% & >=90% (5% of the <<Periodic Payment>>) < 90% & >= 85% (7% of the <<Periodic Payment>>) < 85% & >= 80% (9% of the <<Periodic Payment>>)
2.	Time to Resolve - Severity 1	Time taken to resolve the reported ticket/incident from the time of logging.	For Severity 1, 98% of the incidents should be resolved within 30 minutes of problem reporting	<98% & >=90% (5% of the <<Periodic Payment>>) < 90% & >= 85% (10% of the <<Periodic Payment>>) < 85% & >= 80% (20% of the

#	Service Level Objective	Measurement Methodology /	Target/Service Level	Penalty
				<<Periodic Payment>>)
3.	Time to Resolve - Severity 2,3	Time taken to resolve the reported ticket/incident from the time of logging.	95% of Severity 2 within 4 hours of problem reporting AND 95% of Severity 3 within 16 hours of problem reporting	<95% & >=90% (2% of the <<Periodic Payment>>) < 90% & >= 85% (4% of the <<Periodic Payment>>) < 85% & >= 80% (6% of the <<Periodic Payment>>)
Security Incident and Management Reporting				
1.	Percentage of timely incident report	Measured as a percentage by the number of defined incidents reported within a predefined time (1 hour) limit after discovery, over the total number of defined incidents to the cloud service which are reported within a predefined period (i.e. month). Incident Response - CSP shall assess and acknowledge the defined incidents within 1 hour after discovery.	95% within 1 hour	<95% & >=90% (5% of the <<Periodic Payment>>) < 90% & >= 85% (10% of the <<Periodic Payment>>) < 85% & >= 80% (15% of the <<Periodic Payment>>)
2.	Percentage of timely incident resolutions	Measured as a percentage of defined incidents against the cloud service that are resolved within a predefined time limit (month) over the total number of defined incidents to the cloud service within a	95% to be resolved within 1 hour	<95% & >=90% (5% of the <<Periodic Payment>>) < 90% & >= 85% (10% of the <<Periodic Payment>>) < 85% & >= 80% (15% of the

#	Service Level Objective	Measurement Methodology /	Target/Service Level	Penalty
		predefined period. (Month). Measured from Incident Reports		<<Periodic Payment>>)
Vulnerability Management				
1.	Percentage of timely vulnerability corrections	The number of vulnerability corrections performed by the cloud service provider - Measured as a percentage by the number of vulnerability corrections performed within a predefined time limit, over the total number of vulnerability corrections to the cloud service which are reported within a predefined period (i.e. month). • High Severity Vulnerabilities - 30 days - Maintain 99.95% service level • Medium Severity Vulnerabilities - 90 days - Maintain 99.95% service level	99.95%	>=99% to <99.95% [10% of Periodic Payment] >=98% to <99% [20% of Periodic Payment] <98% [30% of Periodic Payment]
2.	Percentage of timely vulnerability reports	Measured as a percentage by the number of vulnerability reports within a predefined time limit, over the total number of vulnerability reports to the cloud service which are reported within a predefined period (i.e. month).	99.95%	>=99% to <99.95% [10% of Periodic Payment] >=98% to <99% [20% of Periodic Payment] <98% [30% of Periodic Payment]
3.	Security breach including Data Theft /Loss/Corruption	Any incident where in system compromised or any case wherein data theft occurs (including internal incidents)	No breach	For each breach/data theft, penalty will be levied as per following criteria. Any security incident detected

#	Service Level Objective	Measurement Methodology /	Target/Service Level	Penalty
				INR 5 Lakhs. This penalty is applicable per incident. These penalties will not be part of overall SLA penalties cap per month. In case of serious breach of security wherein the data is stolen or corrupted, SSL reserves the right to terminate the contract.
4.	Availability of SLA reports covering all parameters required for SLA monitoring within the defined time		3 working days from the end of the month	5% of <<periodic Payment>>
Service levels for MSP/SI				
1.	Recovery Time Objective (RTO)	Measured during the regular planned or unplanned (outage) changeover from DC to DR or vice versa.	RTO <= 1 hours>	10% of <<Periodic Payment>> per every additional 1 (One) hour of downtime.
2.	Recovery Point Objective (RPO)	Measured during the regular planned or unplanned (outage) changeover from DC to DR or vice versa.	RPO <= 30 mins	10% of <<Periodic Payment>> per every additional 30 mins of downtime
3.	Availability of Root Cause Analysis (RCA) reports for Severity 1 & 2		Average within 5 Working days	5% of <<periodic Payment>>

The severity would be defined as follows:

Severity Level	Description	Examples
Severity 1	Environment is down or major malfunction resulting in an inoperative condition or disrupts critical business functions and requires immediate attention. A significant number of end users (includes public users) are unable to reasonably perform their normal activities as essential functions and critical programs are either not working or are not available.	Non-availability of VM. No access to Storage, software or application
Severity 2	Loss of performance resulting in users (includes public users) being unable to perform their normal activities as essential functions and critical programs are partially available or severely restricted. Inconvenient workaround or no workaround exists. The environment is usable but severely limited.	Intermittent network connectivity
Severity 3	Moderate loss of performance resulting in multiple users (includes public users) impacted in their normal functions.	

4.22 Exit Management

1. Service Provider (SP) shall decommission and withdraw all hardware and software components after the completion of the contract period and formally close the project. This process will be initiated 6 months before the ending of the project contract. In order to align both the parties on transition modalities, Service Provider will submit a detailed Exit Management Plan before 6 months of the ending date of the contract. Exit Management Plan will include following but limited to:
   a. Detailed inventory of all the assets, IT Infrastructure, its location, condition, licenses, documents, manuals, etc. created under the Project.
   b. Method of Transition including roles and responsibilities of both the parties to handover and takeover the charge of project regular activities and support system.
   c. Proposal for necessary setup or institution structure required at SSL level to effectively maintain the project after contract ending.

   d. Training and handholding of SSL Staff or designated officers for maintenance of project after contract ending.

2. SSL will approve this plan after necessary consultation and start preparation for transition.

5. General Conditions of Contract

5.1 General Guidelines

1. The system of recording, measurements and payments will be based on the SSL in vogue.
2. It is presumed that the contractor has gone carefully the standard and special specification of the individual items and studied the site condition before arriving at the percentage above / below the estimated rates quoted by him.
3. Special provisions in the detailed specifications or wording of any item shall give precedence over the corresponding contract provisions, if any. In case of any contradictions in the specifications, the interpretation and decision of the IT in-charge shall be final and binding.
4. If the bidder has any doubts, whatsoever, as to the contents of the contract he is deemed to have in good time i.e. before submitting his tender, get his doubts clarified authoritatively from the Contact Person in writing. Once the tender is submitted by bidder, the matter will be decided according to the tender stipulations.
5. All the time of work in Schedule-B of the tender are completed items of work and no extra claims shall be accepted as regards specifications, infrastructure, all taxes (Sales Tax, GST, etc.), royalties, and any other applicable taxes / charges etc.

6.4 Format to Project Citation

S No	Item	Details	Attachment Ref. Number
1	Name of the Project		
2	Date of Work Order		
3	Client Details		
4	Scope of Work		
5	Contract Value		
6	Completion Date		

Note: The Bidder is required to use above formats for all the projects referenced by the bidder for the Pre-Qualification and technical bid evaluation.

6.5 Project Implementation Methodology

The Bidder is required to submit the proposed technical solution in detail. Following should be captured in the explanation:

a. The Overall approach to the Project
b. Details of Cloud Management Solution
c. A detailed description of the solution and solution approach
d. Implementation Methodology and Overall Solution Architecture and Details Comprising of detailed license requirement for DR setup
e. Strength of the Bidder to provide services including examples or case-studies of similar work
f. Project Organization and Management Plan
g. Project Monitoring and Communication Plan- Bidder's approach to project monitoring and communications among stakeholders
h. Change management methodology
i. The performance benchmark for the offered solution & services
j. The constraints, essentials and necessities if any for installation & commissioning of system
k. Implementation plan- Bidder's approach to implement the project
l. Risk Management Plan - Bidder's approach to identify, respond / manage and mitigate risks
m. Quality Control plan - Bidder's approach to ensure quality of work and deliverables
n. Escalation matrix during contract period
o. Disaster Recovery Plan

Note:

a. All the pages (documentary proofs and other documents that may be attached) should contain page numbers and would have to be uniquely serially numbered.

b. Inadequate information shall lead to disqualification of the bid.

6.6 Check-list for the documents for Pre-Qualification Envelope

A. For Managed Service Provider (MSP) / Cloud Service Provider

6.7 Check-list for the documents for Technical Evaluation

1. Guidelines for Financial Proposal

7.1 Financial Proposal Cover Letter

(To be submitted on the Letterhead of the bidder)

Date: dd/mm/yyyy

To,

HEAD – IT & AUTO
SHCIL Services Limited
SHCIL House, P-51,
TTC Industrial Area,
MIDC, Mahape,
Navi Mumbai - 400710

Subject: Submission of proposal in response to the RFP for Hiring of "Cloud based Disaster Recovery services" from Managed Service Provider

Ref**:** SSL/IT/RFP DC-DR/71

Dear Sir,

We, the undersigned, offer to provide the services for "**Hiring of "Cloud based Disaster Recovery services" from Managed Service Provider "** *in* accordance with your Request for Proposal dated [*Insert Date*] and our Technical Proposal. Our attached Financial Proposal for is for the sum of [*Insert amount(s) in words and figures*]. We are aware that any conditional financial offer will be outright rejected by SSL. Our Financial Proposal shall be binding upon us subject to the modifications resulting from Contract negotiations, up to expiration of the validity period of the Proposal (180 days) from the date of submission of Bid.

We hereby declare that our Tender is made in good faith, without collusion or fraud and the information contained in the Tender is true and correct to the best of our knowledge and belief.

We understand that our Tender is binding on us and that you are not bound to accept a Tender you receive. We confirm that no Pre-Qualification deviations are attached here with this commercial offer. We remain,

Yours sincerely,
Authorized Signature [*In full and initials*]:
Name and Title of Signatory:
Date and Stamp of the signatory
Name of Firm:

7.2 Financial Proposal Instructions

1. SSL may award entire scope or part of scope, mentioned in section 4.0, as SSL deems fit.
2. SSL does not guarantee Work order of any line item in part or whole or volume for the particular line items. The actual volume for the given items may be more or less. The payment shall be made based on unit cost quoted for the particular item on actual services and components is undertaken, and further no extra cost shall be made in any account till the contract period.
3. The bidder should fill rates for all the items mentioned here. If rate for any item is not mentioned then the bid will be rejected by SSL.
4. All the prices are to be entered in Indian Rupees ONLY.
5. The Bidder needs to account for all Out of Pocket expenses due to Boarding, Traveling, Lodging and other related items.
6. The Rates should be exclusive of all taxes. Taxes shall be paid as actual at prevailing rates by SSL at the time of releasing the payments.
7. The rates mentioned above shall be valid for the contract duration.

7.3 Financial Proposal Format

Ref: **SSL/IT/RFP DC-DR/71**

Financial Proposal Format

Table A: Cost Breakdown of Services based on monthly (based on number of hours and days) charges

Sr. No.	Description	Unit	Quantity	Price	Taxes Applicable	Total Cost
Virtual Machines – For Mentioned above applications						
1.	Production Application servers mentioned above	Per Machine per Month				
Storage						
2.	Storage Required as per the mentioned above	3 TB SSD storage per Month (**As per data size**)	1			

Sr. No.	Description	Unit	Quantity	Price	Taxes Applicable	Total Cost
Additional Components						
6.	Additional vCPU	Nos	1			
7.	Additional RAM 4 GB	Nos	1			
8.	Additional RAM 8 GB	Nos	1			
9.	Additional Storage 500 GB	Nos	1			
Software and Licenses – for NSE, ODIN, LD and TradeAnyWhere applications						
10.	OS - Windows Server 2008 R2 Enterprise Edition 64 Bit	Nos				
11.	RDBMS - MS SQL Server	Nos				
Security & Firewall						
12.	Web Application Firewall	Nos	1			
13.	Public IPs (5 IP's to be included at	Nos	1			

Total Cost A1 shall be entered in Summary Table below

Note:

- In case of a particular Instance Type is not available, near or equivalent instance cost to be provided.
- The OS version shall be n, n-1 or a specific version and type as per SSL's Application requirement.
- Bidder has to ensure Cloud Services (VMs provided) should be on Pay per use on hourly, monthly basis and the SSL would pay only for the actual usage.

Table B: Cost towards Support on a yearly basis

Sr. No	Particulars	Per Year Cost	Taxes Applicable	Total Amount
1.	Yearly Support Cost	B1		

Total Cost B1 shall be entered in Summary Table below

Table C: Cost Breakdown for 10 Mbps Connectivity from DC at SSL to DR for 3 years on monthly basis

Sr. No	Particulars	Per Month Cost	Taxes Applicable	Total Amount
1.	10 Mbps Connectivity	C1		

Total Cost C1 shall be entered in Summary Table below

Table D: Consolidated Cost Summary

#	Description	Total Cost excluding taxes for 5 years (in Rs.) (Monthly Cost x 60 / Yearly Cost x 5)	Total Applicable Taxes (in Rs.)	Total Amount (in Rs.)
1.	Cloud Services - Cost for DR environment for 3 years (on demand pricing)(from above table A)	A2=A1 x 60	A3	A = A2 + A3
2.	Cost towards Support from CSP for 3 years (from above table B)	B2=B1 x 5	B3	B = B2 + B3
3.	Cost towards 50 Mbps Connectivity from SSL DC to DR for 3 years (from above table C)	C2=C1 x 60	C3	C = C2 + C3
	Grand Total			GT=A+B+C

Note: Grand Total shall be used for Financial Evaluation

8.

9. ANNEXURES

Annexure A: Format for Declaration by the bidder for not being Blacklisted /Debarred

(To be submitted on the Letterhead of the responding company)

Date: dd/mm/yyyy

To

HEAD-IT & AUTO
SHCIL Services Limited,
SHCIL House, P-51,
TTC Industrial Area,
MIDC, Mahape,
Navi Mumbai —400 710

Subject: Declaration for not being debarred / black-listed by Central / any Government or PSU in India as on the date of submission of the bid

Tender Reference No: SSL/IT/RFP DC-DR/71

Dear Sir,

I, authorized representative of _____ , hereby solemnly confirm that the Company _____ is not debarred /blacklisted by any Government or PSU for any reason as on last date of submission of the Bid. In the event of any deviation from the factual information/ declaration, SSL, Government of Maharashtra reserves the right to reject the Bid or terminate the Contract without any compensation to the Company and forfeiture of Earnest Money Deposit and/or Security Deposit

Thanking you,

Yours faithfully,

Signature of Authorized Signatory (with official seal) Date:
Name:
Designation:
Address:
Telephone &Fax:

E-mail address:

Annexure B: Performance Security - Bank Guarantee Format

For Contract Performance Bank Guarantee

Ref: **SSL/IT/RFP DC-DR/71**

Date: _____

Bank Guarantee No.: _____

To

HEAD-IT & AUTO
SHCIL Services Limited,
SHCIL House, P-51,
TTC Industrial Area,
MIDC, Mahape,
Navi Mumbai —400 710

Dear Sir,

Annexure C: Non-Disclosure Agreement

[Company Letterhead]

This AGREEMENT (hereinafter called the "Agreement") is made on the [day] day of the month of [month], [year], between, SHCIL Services Ltd on the one, (hereinafter called the "SSL") and, on the other hand, [Name of the Bidder] (hereinafter called the "Bidder") having its registered office at [Address]

WHEREAS

1. The "SSL" has issued a public notice inviting various organizations for provision of Hiring of "Cloud based Disaster Recovery Services" from Managed Service Provider at SHCIL Services Ltd(SSL) , Mumbai (hereinafter called the "Project") of the SSL;

2. The Bidder, having represented to the "SSL" that it is interested to bid for the proposed Project,

3. The SSL and the Bidder agree as follows:

a) In connection with the "Project", the SSL agrees to provide to the Bidder a

detailed document on the Project vide the Request for Proposal document. The Request for Proposal contains details and information of the SSL operations that are considered confidential.

b) The Bidder to whom this information (Request for Proposal) is disclosed shall

i. hold such information in confidence with the same degree of care with which the Bidder protects its own confidential and proprietary information;
ii. restrict disclosure of the information solely to its employees, other member with a need to know such information and advice those persons of their obligations hereunder with respect to such information;
iii. use the information only as needed for the purpose of bidding for the Project;
iv. except for the purpose of bidding for the Project, not copy or otherwise duplicate such information or knowingly allow anyone else to copy or otherwise duplicate such information; and
v. undertake to document the number of copies it makes
vi. on completion of the bidding process and in case unsuccessful, promptly return to the SSL, all information in a tangible form or destroy such information

4. The Bidder shall have no obligation to preserve the confidential or proprietary nature of any information which:

a) was previously known to the Bidder free of any obligation to keep it confidential at the time of its disclosure as evidenced by the Bidder's written records prepared prior to such disclosure; or
b) is or becomes publicly known through no wrongful act of the Bidder; or
c) is independently developed by an employee, agent or contractor of the Bidder not associated with the Project and who did not have any direct or indirect access to the information.

5. The Agreement shall apply to all information relating to the Project disclo sed by the SSL to the Bidder.

6. SSL will have the right to obtain an immediate injunction enjoining any breach of this Agreement, as well as the right to pursue any and all other rights and remedies available at law or in equity for such a breach.

7. SSL reserves the right to share the information received from the bidder under the ambit of RTI Act.

8. Nothing contained in this Agreement shall be construed as granting or conferring rights of license or otherwise, to the Bidder, on any of the information. Notwithstanding the disclosure of any information by the SSL to the Bidder, the SSL shall retain title and all intellectual property and proprietary rights in the information. No license under any

trademark, patent or copyright, or application for same that are now or thereafter may be obtained by the SSL is either granted or implied by the conveying of information. The Bidder shall not alter or obliterate any trademark, trademark notice, copyright notice, confidentiality notice or any notice of any other proprietary right of the SSL on any copy of the information, and shall reproduce any such mark or notice on all copies of such information.

9. This Agreement shall be effective from the date of signing of this agreement and shall continue perpetually.

10. Upon written demand of the SSL, the Bidder shall (i) cease using the information, (ii) return the information and all copies, notes or extracts thereof to the SSL forthwith after receipt of notice, and (iii) upon request of the SSL, certify in writing that the Bidder has complied with the obligations set forth in this paragraph.

11. This Agreement constitutes the entire Agreement between the SSL and the Bidder relating to the matters discussed herein and supersedes any and all prior oral discussions and/or written correspondence or agreements between the two 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.

12. Confidential information is provided "As-Is". In no event shall the SSL be liable for the accuracy or completeness of the confidential information.

13. This agreement shall benefit and be binding upon the SSL and the Bidder and their respective subsidiaries, affiliate, successors and assigns.

14. This agreement shall be governed by and construed in accordance with the Indian laws.

For and on behalf of the Bidder (Signature)
(Name of the authorized Signatory) Designation :

Date :

Time :

Seal :

Business Address

Annexure D: Declaration of Data Security

To,
HEAD-IT & AUTO
SHCIL Services Limited,
SHCIL House, P-51,
TTC Industrial Area,
MIDC, Mahape,
Navi Mumbai —400 710
Dear Sir,

We..... who are established and reputable bidder having office at..... do hereby certify that SSL shall have absolute right on the digital data and output products processed / produced by us. We shall be responsible for security / safe custody of data during processing.

We also certify that the data will not be taken out of the SSL's premises on any media. The original input data supplied to us by SSL and output products processed / produced from input data will not be passed on to any other Service Provider (SP) or individual other than the authorized person of SSL. We shall abide by all security and general instructions issued by SSL from time to time.

We also agree that any data from our computer system will be deleted in the presence of SSL official after completion of the project task.

Thanking you,

Yours faithfully,

Annexure E: Power of Attorney

Know by all men by these presents, We _____ (Name of the Bidder and address of their registered office) do hereby constitute, appoint and authorize Mr. / Ms _____ (name and residential address of Power of attorney holder) who is presently employed with us and holding the position of _____ as our Attorney, to do in our name and on our behalf, all such acts, deeds and things necessary in connection with or incidental to our Proposal for the **"Request for Selection for Hiring of "Cloud based Disaster Recovery services" from Managed Service Provider at SHCIL Services Ltd(SSL)"**, including signing and submission of all documents and providing information / responses to the SSL, representing us in all matters before SSL, and generally dealing with the SSL in all matters in connection with our Proposal for the said Project.

We hereby agree to ratify all acts, deeds and things lawfully done by our said Attorney pursuant to this Power of Attorney and that all acts, deeds and things done by our aforesaid Attorney shall and shall always be deemed to have been done by us.

For
Name:
Designation:
Date:
Time:
Seal:
Business Address:

Accepted,
_____ (Signature)
(Name, Title and Address of the Attorney)

Note:

- The mode of execution of the Power of Attorney should be in accordance with the procedure, if any, laid down by the applicable law and the charter documents of the executant(s) and when it is so required the same should be under common seal affixed in accordance with the required procedure.
- The Power of Attorney shall be provided on Rs.100/- stamp paper.
- The Power of Attorney should be supported by a duly authorized resolution of the Board of Directors of the Bidder authorizing the person who is issuing this power of attorney on behalf of the Bidder.

Annexure F: Agreement Format

THIS AGREEMENT made the..... day of .....2019 BETWEEN SHCIL Services Limited having its office at SHCIL House, P-51, TTC Industrial Area, MIDC, Mahape, Navi Mumbai —400 710 (hereinafter referred to as "SSL") which expression shall unless repugnant to the context or meaning thereof mean and be deemed to include its authorized agents, representatives and permitted assigns of the First Part.
AND

M/s <Name of the Bidder>having its office at <office address of the bidder> which expression shall unless repugnant to the context or meaning thereof mean and be deemed to include their successors and permitted assigns of the Second Part.

WHEREAS the contractor has tendered for providing services to SSL as per the terms and conditions mentioned in the Request for Proposal (from herein after referred to as "RFP") "For Hiring of "Cloud based Disaster Recovery Services" from Managed Service Provider for SHCIL Services Ltd (SSL)" dated <date of release of RFP> and the all subsequent corrigendum's published document, as per the Commercial Bid submitted in response to the RFP dated <date of release of RFP >. Whereas such tender has been accepted and the contractor has provided Bank Guarantee to SSL, Mumbai for the sum of Rs. <amount of the bid>.

NOW IT IS HEREBY AGREED between the parties hereto as follows:
The contractor has accepted the contract on the terms and conditions set out in the RFP No: <Ref no of RFP> issued on <date of issue of RFP> and all subsequent communications through letters / emails and clarifications/corrigendum issued which shall hold good during period of this agreement.

Refund of deposit shall be based on the timelines, terms and conditions as has been specified in the RFP/LoI and shall form a part of the contract. In absence of any timeline specified the deposit shall after the expiration of 180 days from the date of completion of the contract, be returned to the contractor but without interest and after deducting there from any sum due by the contractor to SSL under the terms and conditions of this agreement.

This agreement shall remain in force until the expiry of <duration of the contract> from the date of entering into the contract, but SSL may cancel the contract at any time upon giving 30 days' notice in writing without compensating the Service Provider.

All terms and conditions as specified in the RFP, clarifications / corrigendum issued in regards to the RFP <ref no RFP> as has been mentioned above in the document shall stand enforce unless has been expressly agreed to in writing by both the parties.
The Contractor shall be responsible to abide and shall be liable to deliver the requirements/deliverables as has been specified to in the RFP, clarifications / corrigendum issued in regards to the RFP. No. <ref no RFP> and Letter of Acceptance No: <LoI number> dated <date>.

IN WITNESS whereof the said Contractor hath set his hand hereto and SSL has affixed his hand and seal thereto the day and year first above written.

Signed, sealed and delivered By HEAD - IT & AUTO For and on behalf of SHCIL Services Ltd Witnesses: (1) (2)	Signed, sealed and delivered By For and on behalf of M/s <Name of Bidder> Witnesses: (1) (2)

End of Document*