HLL Lifecare Limited
(A Government of India Enterprise)

एचएलएल लाइफ़केयर लिमिटेड
(भारत सरकार का उद्यम)

Request for Proposal
For
Installation, Configuration and Maintenance of Cloud Based Infrastructure for HLL

E-Tendering

CONTENTS

HLL LIFECARE LIMITED
(A Government of India Enterprise)
Corporate and Registered, Poojappura.P.O,
Thiruvananthapuram – 695012, Kerala, India
Phone: 0471- 2354949, 2775500

NOTICE INVITING TENDER (NIT)

IFB No: HLL/CHO/IT/CI/2023 **08-02-2023**

To,
____
____

Dear Sir,

HLL Lifecare Limited (HLL) a Govt. of India Enterprise under the Ministry of Health and Family Welfare invites proposals for the Installation, Configuration and Maintenance of Cloud Based Infrastructure for hosting the SAP Applications of HLL. More details on the services are provided in the Schedule of Requirements.

Bid documents can be downloaded free of cost from the Government e-procurement portal (URL: https://etenders.gov.in/eprocure/app). However, tender document fees shall be payable at the time of bid submission as stipulated in this tender document. All corrigendum/extension regarding this e-tender shall be uploaded on this portal i.e. https://etenders.gov.in/eprocure/appand shall not be available elsewhere.

You are requested to go through the document carefully and submit your proposals as per the instructions and guidelines given in the tender document.

Yours sincerely,

Associate Vice President (IT),
HLL Lifecare Limited, Corporate and Registered office,
HLL Bhavan, Poojappura P.O,
Thiruvananthapuram, Kerala -695012
Phone No: – 0471-2775500, 2354949.
Email address: erp@lifecarehll.com

Important Information

Sl No	Particulars	Description
1	Tender Inviting Authority	HLL Lifecare Limited
2	Office Address	HLL Lifecare Limited Corporate and Registered Office HLL Bhavan, Poojappura P.O Thiruvananthapuram, Kerala 695012
3	RFP/ Bid Number	HLL/CHO/IT/CI/2023
4	Name of work	Installation, Configuration and Maintenance of Cloud Based Infrastructure for hosting the SAP Applications of HLL
5	Brief description of Item/Work	1. Design, Installation and Configuration of Cloud based Infrastructure for SAP Applications as mentioned in Annexure 1. 2. Maintenance of Cloud infrastructure for 3 Years.
6	Bid Security/EMD	**Rs.6,00,000/- (Rs. Six Lakh only)** (Note: In case of MSE or Start-up who are eligible for EMD exemption should provide a Bid Security Declaration is to be attached in the format given in the tender).
7	Bid Submission Fee/Tender Fee (nonrefundable, shall be submitted separately)	Rs. 5,000/- (including GST @ 18%)
8	Period of completion for the work	6 Weeks from the date of issue of work order.
9	Eligibility criteria for Bidders	As per the Tender document
10	Last Date for Submission of pre-bid queries by bidders (by email in the prescribed form)	15.02.2023 17:00 Hrs. IST
12	Bid submission start date	17.02.2023
13	Last date and time for online submission of bids	01.03.2023 at 17:00 hrs.
14	Date and time of opening of e-tender	03.03.2023 at 10:30 hrs.
15	HLL A/c details for payment of Tender Fees (Payment mode: NEFT/RTGS)	Name of Bank : State Bank of India A/c number : 10183256222 IFSC Code : SBIN0004350 Branch name : Commercial Branch, Thiruvananthapuram

Disclaimer

The information contained in this document is confidential in nature. The bidders shall not share this information with any other party not connected with responding to this Tender Document. All information contained in this Request for Proposal (RFP) provided / clarified are in good interest and faith. This is not an agreement and is not an offer or invitation to enter into an agreement of any kind with any party.

The information contained in this Tender Document or subsequently provided to Bidder(s) whether verbally or in writing by or on behalf of HLL Lifecare Limited (HLL) shall be subject to the terms and conditions set out in this Tender Document and any other terms and conditions subject to which such information is provided.

Though adequate care has been taken in the preparation of this RFP document, the interested firms shall satisfy themselves that the document is complete in all respects. The information is not intended to be exhaustive. Interested Bidders are required to make their own enquiries and assumptions wherever required. Intimation of discrepancy, if any, should be given to the specified office immediately. If no intimation is received by this office by the date mentioned in the document, it shall be deemed that the RFP document is complete in all respects and firms submitting their bids are satisfied that the RFP document is complete in all respects.

If a bidder needs more information than what has been provided, the potential bidder is solely responsible to seek the information required from HLL. HLL reserves the right to provide such additional information at its sole discretion. In order to respond to the Bid, if required, and with the prior permission of HLL, each bidder may conduct his own study and analysis, as may be necessary.

HLL Lifecare limited (HLL), Thiruvananthapuram reserves the right to reject any or all of the applications submitted in response to this RFP document at any stage without assigning any reasons whatsoever. HLL also reserves the right to withhold or withdraw the process at any stage with intimation to all who submitted the RFP Application. HLL reserves the right to change/modify/amend any or all of the provisions of this RFP document. Such changes would be posted on the e-portal of Central Public Procurement Portal of Government of India i.e. https://etenders.gov.in/eprocure/app

Neither HLL nor their employees and associates will have any liability to any prospective respondent interested to apply or any other person under the law of contract, to the principles of restitution or unjust enrichment or otherwise for any loss, expense or damage which may arise from or be incurred or suffered in connection with anything contained in this RFP document, any matter deemed to form part of this RFP document, the award of the Assignment, the information and any other information supplied by or on behalf of HLL or their employees and Bidder or otherwise arising in any way from the selection process for the Assignment.

Part – I

Introduction

1. INTRODUCTION

HLL Lifecare Limited (HLL) formerly known as Hindustan Latex Ltd is a Mini Ratna Govt. of India Enterprise, under the Ministry of Health & Family Welfare. HLL was established in 1966 to manufacture and supply condoms to the National Family Planning Programme of Govt. of India.

HLL has traversed a long path, over the past fifty six years. From a single product company, HLL has emerged as a multiproduct, multi-location Company with a wide range of healthcare products and services. The foundation of HLL's legacy is its focus on high quality and affordable costs. At present, HLL has 7 state-of-the art manufacturing facilities and 22 regional offices across India. HLL is also one of the leading social marketing organisations in the country in the area of contraceptives - with a market share of over 70 percent in the rural and semi urban markets. On the global front, HLL brands today reach more than 115 countries.

Besides establishing its credentials as a dependable supplier of contraceptives and healthcare products HLL is the preferred implementation partner for many of the Government projects, especially in the areas of medical diagnostics services, running of maternity & child hospitals and sale of generic drugs and medical devices through fair-price shops.

HLL Products

HLL is one of the leading producers of contraceptives in the world. The range includes Male Condoms, Female condoms, Intra-Uterine Devices, Oral Contraceptive Pills- Steroidal and Non-steroidal, Emergency Contraceptive Pills, Tubal Rings and Injectables. MOODS is the commercial condom brand of HLL and comes with 19 variants, appealing to customer segments across different age groups. Besides, HLL has a vast array of innovative healthcare products and services, ranging from Blood Bags to Blood Banking Equipment, Surgical Sutures to Surgical Gloves, and Equipment for Neonatal Care. HLL has been able to reach out and save millions of lives across the world, using its Blood Transfusion Service Equipment and Wound Care (WC) products. HLL also manufactures Rapid Diagnostic Test Kits, various Pharma Products for Women, Sanitary Napkins, Menstrual Cups, Vending Machines, Incinerators, Deodorants, Lubes, Medicated Plasters, Oral Re-hydration Salts and a range of Covid management products such as Automatic sanitizer dispensing machine, UV sanitizing box , Mediguard Hand Sanitizer, Mask cum Sanitizer vending machine.

Health Care Services (HCS)

Established under the brand name, **HINDLABS** is a network of state-of-the- art diagnostic centers and clinical laboratories across India. It offers the most comprehensive and advanced imaging and laboratory services at the most affordable prices for the general public. HINDLABS offers:

- Clinical Lab services - includes Hematology, Biochemistry, Pathology, Immunoassay, Microbiology & special tests
- Radio diagnostic imaging services - MRI Scan, CT Scan, X-Ray (Digital / CR System /conventional), 3D/4D Ultrasound, Mammography, BMD, OPG and Dental X-Ray etc.

Currently, **HINDLABS** has a chain of 279 diagnostic centers established across 13 states in India providing affordable diagnostic services, thereby reducing the huge out-of-pocket expenses incurred by the general public.

Retail Pharmacy Services

In 2015, HLL ventured into Pharma retailing. The division operates a retail chain of pharmacies offering quality pharmaceuticals, medicines, and implants to the common man at affordable prices. **AMRIT (Affordable Medicines and Reliable Implants for Treatment),** an initiative of MoHFW is a network of pharmacies offering more than 5200 drugs, implants, surgical disposables, and other consumables at average discounts of up to 40% of the Maximum Retail Price (MRP). Today, AMRIT has a Pan-India presence across 28 states/ Union territories providing pharmacy services through 233 retail outlets.

HLL has also partnered with the state governments in spreading awareness among girl students regarding menstrual hygiene and health, supported by corporate social responsibility funds of various corporations.

Procurement and distribution of COVID-19 emergency medical supplies

In March 2020, during the emergence of COVID-19 pandemic in India, the Ministry of Health & Family Welfare (MoHFW) nominated HLL as the Nodal Agency for the Procurement and supply of Emergency Medical items to fight against the pandemic. HLL took up this mammoth task in a project mode and executed the same by building an institutional mechanism to handle the procurement and distribution of emergency supplies across India. The products covered PPE coveralls, N 95 masks, Goggles, Ventilators, Oxygen concentrators, Nitrile gloves and vaccines. With a wider spectrum of activities, HLL touches the lives of millions across the world thereby rightly realising its motto of '**Innovating for Healthy Generations**'.

HLL's subsidiary / associate companies:

1. HLL Infra Tech Services Limited (HITES) for hospital infrastructure development
2. Hindustan Latex Family Planning Promotion Trust, a not-for-profit trust engaged in Social Marketing,
3. LifeSpring Hospitals a JV with Acumen Fund USA offering for maternity care services in the state of AP
4. Goa Antibiotics and Pharmaceuticals Limited (GAPL)
5. HMA – HLL Management Academy
6. HLL Pratheeksha Charitable Society

2. <u>SAP – OVERVIEW IN HLL</u>

HLL's Data Center (DC) resides at our Corporate & Registered Office premise in Thiruvananthapuram and Disaster Recovery (DR) site hosted and managed by M/s CtrlS Datacenters Ltd at Hyderabad. HLL has gone live with the SAP-ERP solution in August 2011.

Part – II

General Instructions to Bidders

General Instructions to Bidders

1. This tender is an e-Tender and is being published online in Government e-Procurement portal, https://etenders.gov.in/eprocure/app

2. Bid documents including the Bill of Quantities (BOQ) can be downloaded free of cost from the Central Public Procurement Portal of Government of India (e-portal). All Corrigendum/extension regarding this e-tender shall be uploaded on this website i.e. https://etenders.gov.in/eprocure/app.

3. The tendering process is done online only at Government eProcurement portal (URL address: https://etenders.gov.in/eprocure/app). Aspiring bidders may download and go through the tender document.

4. All bid documents are to be submitted online only and in the designated cover(s)/envelope(s) on the Government eProcurement website. Tenders/bids shall be accepted only through online mode on the Government eProcurement website and no manual submission of the same shall be entertained. Late tenders will not be accepted.

5. The complete bidding process is online. Bidders should be in possession of valid Digital Signature Certificate (DSC) of class II or above for online submission of bids. Prior to bidding DSC need to be registered on the website mentioned above. If the envelope is not digitally signed & encrypted the Purchaser shall not accept such open Bids for evaluation purpose and shall be treated as non-responsive and rejected.

6. Bidders are advised to go through “Bidder Manual Kit”, “System Settings” & “FAQ” links available on the login page of the e-Tender portal for guidelines, procedures & system requirements. In case of any technical difficulty, Bidders may contact the help desk numbers & email ids mentioned at the e-tender portal.

7. Bidders are advised to visit CPPP website https://etenders.gov.in regularly to keep themselves updated, for any changes/modifications/any corrigendum in the Tender Enquiry Document.

8. The bidders are required to submit soft copies of their bids electronically on the CPP Portal, using valid Digital Signature Certificates. The instructions given below are meant to assist the bidders in registering on the CPP Portal, prepare their bids in accordance with the requirements and submitting their bids online on the Government eProcurement Portal.

8.1 Registration

a) Bidders are required to register in the Government e-procurement portal, obtain 'Login ID' & 'Password' and go through the instructions available in the Home page after log in to the CPP Portal (URL: https://etenders.gov.in/eprocure/app), by clicking on the link "Online bidder Enrolment" on the CPP Portal which is free of charge.

b) As part of the enrolment process, the bidders will be required to choose a unique user name and assign a password for their accounts.

c) Bidders are advised to register their valid email address and mobile numbers as part of the registration process. These would be used for any communication from the CPP Portal.

d) They should also obtain Digital Signature Certificate (DSC) in parallel which is essentially required for submission of their application. The process normally takes 03 days' time. The bidders are required to have class-2 digital certificate or above with both signing and encryption from the authorized digital signature Issuance Company. Please refer online portal i.e. -https://etenders.gov.in/eprocure/appfor more details.

e) Upon enrolment, the bidders will be required to register their valid Digital Signature Certificate (Class II or above Certificates with signing key usage) issued by any Certifying Authority recognized by CCA India (e.g. Sify /nCode / eMudhra etc.), with their profile.

f) Bidder then logs in to the site through the secured log-in by entering their user ID/password and the password of the DSC / e-Token.

g) The Bidder intending to participate in the bid is required to register in the e-tenders portal using his/her Login ID and attach his/her valid Digital Signature Certificate (DSC) to his/her unique Login ID. He/She has to submit the relevant information as asked for about the firm/contractor. The bidders, who submit their bids for this tender after digitally signing using their Digital Signature Certificate (DSC), accept that they have clearly understood and agreed the terms and conditions including all the Forms/Annexure of this tender.

h) Only those bidders having a valid and active registration, on the date of bid submission, shall submit bids online on the e-procurement portal.

i) Only one valid DSC should be registered by a bidder. Please note that the bidders are responsible to ensure that they do not lend their DSC's to others which may lead to misuse.

j) Ineligible bidder or bidders who do not possess valid & active registration, on the date of bid submission, are strictly advised to refrain themselves from participating in this tender.

8.2 Searching for Tender Documents

a) There are various search options built in the CPP Portal, to facilitate bidders to search active tenders by several parameters. These parameters could include Tender ID, Organization Name, Form of Contract, Location, Date, Value etc. There is also an option of advanced search for tenders, wherein the bidders may combine a number of search parameters such as Organization

b) Once the bidders have selected the tenders they are interested in, they may download the required documents/tender schedules. These tenders can be moved to the respective 'My Tenders' folder. This would enable the CPP Portal to intimate the bidders through SMS/ e-mail in case there is any corrigendum issued to the tender document.

c) The bidder should make a note of the unique Tender ID assigned to each tender, in case they want to obtain any clarification/help from the Helpdesk.

8.3 Preparation of Bids

a) Bidder should take into account any corrigendum published on the tender document before submitting their bids.

b) Please go through the tender document carefully to understand the documents required to be submitted as part of the bid. Please note the number of covers in which the bid documents have to be submitted, the number of documents - including the names and content of each of the document that need to be submitted. Any deviations from these may lead to rejection of the bid.

c) Bidder, in advance, should get ready the bid documents to be submitted as indicated in the tender document / schedule and generally, they can be in PDF / XLS / RAR /DWF/JPG formats. Bid documents may be scanned with 100 dpi with black and white option which helps in reducing size of the scanned document.

d) To avoid the time and effort required in uploading the same set of standard documents which are required to be submitted as a part of every bid, a provision of uploading such standard documents (e.g. PAN card copy, annual reports, auditor certificates etc.) has been provided to the bidders. Bidders can use "My Space" or ''Other Important Documents'' area available to them to upload such documents. These documents may be directly submitted from the "My Space" area while submitting a bid, and need not be uploaded again and again. This will lead to a reduction in the time required for bid submission process.

e) Note: My Documents space is only a repository given to the Bidders to ease the uploading process. If Bidder has uploaded his Documents in My Documents space, this does not automatically ensure these Documents being part of Technical Bid.

9. More information useful for submitting online bids on the CPP Portal may be obtained at https://etenders.gov.in/eprocure/app

10. Tenderer are required to upload the digitally signed file of scanned documents. Bid documents may be scanned with 100 dpi with black and white option which helps in reducing size of the scanned document. Uploading application in location

other than specified above shall not be considered. Hard copy of application shall not be entertained.

11. Any queries relating to the process of online bid submission or queries relating to CPP Portal in general may be directed to the 24x7 CPP Portal Helpdesk. The 24x7 Help Desk details are as below: -

    For any technical related queries please call at 24 x 7 Help Desk Number:

    0120-4001 062, 0120-4001 002, 0120-4001 005, 0120-6277 787

    Note:- International Bidders are requested to prefix +91 as country code

    E-Mail Support: For any Issues or Clarifications relating to the published tenders, bidders are requested to contact the respective Tender Inviting Authority

    Technical - support-eproc@nic.in, Policy Related - cppp-doe@nic.in

12. Bidders are requested to kindly mention the URL of the portal and Tender ID in the subject while emailing any issue along with the contact details.

Any queries relating to the tender document and the terms and conditions contained therein should be addressed to the Tender Inviting Authority for a tender or the relevant contact person indicated in the tender. Address for communication and place of opening of bids:

Associate Vice President (IT),
HLL Lifecare Limited, Corporate and Registered office,
HLL Bhavan, Poojappura P.O,
Thiruvananthapuram, Kerala -695012
Phone No: – 0471-2775500, 2354949.
Email address: erp@lifecarehll.com

13. The bids shall be opened online at the **Office of the Associate Vice President (IT).** If the tender opening date happens to be on a holiday or non-working day due to any other valid reason, the tender opening process will be done on the next working day at same time and place.
14. More details can be had from the Office of the **Associate Vice President (IT)** during working hours. HLL shall not be responsible for any failure, malfunction or

breakdown of the electronic system while downloading or uploading the documents by the Bidder during the e-procurement process.

15. A bidder shall submit only one bid in the same bidding process. A Bidder who submits or participates in more than one bid will cause all the proposals in which the Bidder has participated to be disqualified.

16. Joint ventures or Consortiums of bidders are not permitted.

17. Online Tender process

The tender process shall consist of following stages:

i. Downloading of tender document: Tender document will be available for free download on Government e-procurement portal (URL: https://etenders.gov.in/eprocure/app). However, tender document fees shall be payable at the time of bid submission as stipulated in this tender document.

ii. Publishing of Corrigendum: All corrigenda shall be published on Government e-procurement portal (URL: https://etenders.gov.in/eprocure/app) and shall not be available elsewhere.

iii. Bid submission: Bidders have to submit their bids along with supporting documents to support their eligibility, as required in this tender document on Government e-procurement portal. No manual submission of bid is allowed and manual bids shall not be accepted under any circumstances.

iv. Opening of Technical Bid and Bidder short-listing: The technical bids will be opened, evaluated and shortlisted as per the eligibility and technical qualifications. All documents in support of technical qualifications shall be submitted (online). Failure to submit the documents online will attract disqualification. Bids shortlisted by this process will be taken up for opening the financial bid.

v. Opening of Financial Bids: Bids of the qualified bidders shall only be considered for opening and evaluation of the financial bid on the date and time mentioned in critical date's section.

18. Tender Document Fees

Tender fee (Non-refundable) as per the tender conditions shall be paid separately, through RTGS/NEFT transfer in the following HLL A/c details:

Name of Bank:	State Bank of India
A/c number:	10183256222
IFSC Code:	SBIN0004350
Branch name:	Commercial Branch, Thiruvananthapuram

Document of the above transactions completed successfully by the bidder, shall be uploaded at the locations separately while submitting the bids online.

Bid Security Declaration is to be attached in the format (Form A9) given in this document.

Note: Any transaction charges levied while using any of the above modes of payment has to be borne by the bidder. The bids will be evaluated only if payment is effective on the date and time of bid opening.

19. HLL Lifecare Limited does not bind themselves to accept the lowest or any bid or to give any reasons for their decisions which shall be final and binding on the bidders.

20. HLL Lifecare Limited reserves to themselves the right of accepting the whole or any part of the tender and bidder shall be bound to perform the same at his quoted rates.

21. In case, it is found during the evaluation or at any time before signing of the contract or after its execution and during the period of subsistence thereof, that one or more of the eligibility conditions have not been met by the bidder or the applicant has made material misrepresentation or has given any materially incorrect or false information, appropriate legal/penal etc., action shall be taken by HLL Lifecare Limited including but not limited to forfeiture of EMD, Security Deposit etc., as deemed fit by HLL Lifecare Limited.

22. Conditional bids and bids not uploaded with appropriate/desired documents may be rejected out rightly and decision of HLL Lifecare Limited in this regard shall be final and binding.

23. The bidder should comply all statutory obligation in force and amended from time to time and HLL Lifecare Limited will not be held responsible in any manner whatsoever for any non-compliance of statutory obligations by the bidder.

24. The technical bids should be uploaded as per the requirements of NIT and should not contain price information otherwise the bid will be rejected.

25. HLL Lifecare Limited Ltd. reserves the right to verify the claims made by the bidders and to carry out the capability assessment of the bidders and the HLL Lifecare Limited's decision shall be final in this regard.

26. Submission Process:

For submission of bids, all interested bidders have to register online as explained above in this document. After registration, bidders shall submit their Technical bid and Financial bid online on Government e-procurement portal (URL: https://etenders.gov.in/eprocure/app) along with tender document fees and EMD.

Note:- It is necessary to click on "Freeze bid" link/ icon to complete the process of bid submission otherwise the bid will not get submitted online and the same shall not be available for viewing/ opening during bid opening process.

Part – III

General Conditions of Contract

General Conditions of Contract

General conditions of contract are broad guidelines to be followed while formulating the bid and its submission to the Purchaser. It also describes the methodology for opening and evaluation of bids and consequent award of contract.

1. DEFINITIONS

In this Contract, the following words and expressions shall have the meanings as stated below:

a. **'Invitation for Bid'** shall mean and include the present document, and such other complements and agenda, which may subsequently be issued in this connection.

b. **'Bidder/Tenderer'** shall mean the person, firm or Corporation submitting a bid against this invitation for bid and shall also include his agents and representatives.

c. **'Purchaser/Owner'** shall mean HLL Lifecare Limited (HLL) (Thiruvananthapuram) or its units thereof.

d. **'Acceptance Letter'**, shall mean written consent by a letter of purchaser/owner to the bidder intimating him that his tender has been accepted.

e. **'Date of Contract'**, shall mean the date of issue of Notification of Award.

f. **'Contract Period'**, shall mean the period specified in the tender documents during which the contract shall be executed.

g. **'Completion Certificate'**, shall mean the certificate issued by the purchaser/owner to the Bidder after successful completion of the project.

h. **'Managed Service Provider (MSP)'**, shall mean the successful bidder who install, configure and maintain the Cloud based Services from **Cloud Service Provider (CSP)**.

i. **'Personnel'** means professional and support staff provided by the bidder

j. **‘Third Party’** means any person or entity other than the HLL and the Bidder

k. **‘Maintenance’** shall mean and include the support as mentioned under Scope of Work.

2. SCOPE OF THE BID

HLL invites online bids for the Installation, Configuration and Maintenance of Cloud based Infrastructure for its SAP Applications from eligible, competent and experienced parties who are capable of executing the specified works per our tender conditions. The detailed scope of work is given under the heading Part –IV (Scope of Work) of this document.

3. ELIGIBILITY CRITERIA

- The bidder shall be System Integrator (SI) only with due authorization from respective CSP.
- MSP cannot have a consortium with another MSP. All the required services must be provided through a single CSP only.
- CSP alone can also bid, if it meets the eligibility criteria for both MSP and CSP.
- The bidders shall not have a conflict of interest that affects the Bidding Process.
- The bidder should clearly indicate the compliance towards each requirement as per the table furnished in Form A6 of this document.
- A bidder shall submit only one bid in the same bidding process. A Bidder (either as a firm or as a partner of a firm) who submits or participates in more than one bid will cause all the proposals in which the Bidder has participated to be disqualified
- The bidders should also upload/ submit the valid documentary proof or respective certificates as mentioned in the prequalification compliance form as mentioned in Form A3 of this document.

3.1 Eligibility of the Bidder/ Managed Service Provider (MSP):

The prospective bidder should satisfy the following criterion.

Sl.No	Criteria	Docs Requested
1	The bidder shall be a Indian Company/Firm in continuous business of the Hosting & Maintenance of Cloud infrastructure for the last Five (5) Years and registered under either ; • The Indian Companies Act, 2013 OR • A partnership firm registered under the Limited Liability Partnerships (LLP) Act, 2008 OR • A partnership firm registered under the Indian Partnership Act, 1932.	Copy of valid Certificate of Incorporation or Certified copy of valid Partnership Deed.
2	The bidder should have all the following Experience in India during the last Five (5) Years prior to the Bid Submission Date; • Minimum **Five** (5) successful implementation of Cloud Environment. • Minimum **One** (1) successful implementation of Cloud Environment with order value greater than Rs. 50 Lakh **or** Minimum Two (2) successful implementations of Cloud Environment with order value greater than Rs. 25 Lakh. • Minimum **Two** (2) Nos. of successful implementations of Cloud Environment in PSU/Central Govt/State Govt. • Minimum **One** (1) No. successful implementation of Cloud Environment for SAP Applications (ECC/S4HANA)	Documentary evidences like Work Orders, Installation Certificates, and Client Certificate etc. for the same should be attached along with the bid.
3	The Bidder should have minimum average annual turnover of Rs. 50 Crores from IT Services during the last three Financial Years. i.e. (2019-20, 2020-21 and 2021-22).	Audited Balance Sheets and Profit & Loss account for the last three financial years and certificate from the statutory auditor shall be submitted. If the turnover is from fields other than IT services, then certificate from

		statutory auditor to be submitted for turnover from IT services separately (Supported with Form A6 certified by statutory auditor).
4	The bidder should not have been blacklisted in past three years by any State/Central Government Organizations / Firms / Institutions	Self-certificate stating that the bidder has not been blacklisted by any institution of the Central /State Government
5	The bidder should be regular tax payer under the Income Tax Act.	Details of PAN, GST etc.
6	The bidder should have at least 10 Nos. of Professionals with certifications of the proposed Cloud Service Provider.	Details of such 10 Nos. of professionals shall be attached along with the bid.
7	The bidder should have certified for ISO 9001, ISO 20000 and ISO 27001.	Documentary evidences for the same should be attached along with the bid
8	The bidder should be an authorized partner of the proposed Cloud Service Provider.	Authorization letter from the quoted CSP shall be submitted along with the bid.

3.2. Eligibility of the Proposed Cloud Service Provider (CSP):

Sl.No	Criteria	Docs Requested
1	Proposed CSP should be an Indian Company registered under the Indian Companies Act, 2013.	Copy of valid Certificate of Incorporation
2	Proposed CSP and offered facilities for DC&DR should have been ; • Empaneled by Ministry of Electronics and Information Technology (MeitY) for the last 3 years. And • STQC audited as per MeitY empanelment process as on the last date of submission of the bid.	Self-certified copy of MeitY, Government of India empanelment as CSP.

3	Proposed CSP should have accreditations relevant to security, availability, confidentiality, processing integrity, and privacy Trust Services principles SOC 1, SOC 2 and SOC 3	Self-declaration from the Authorized signatory of the CSP on their letterhead.
4	CSP must not have been blacklisted by a Central & State Government Institution/PSUs in India.	Self-declaration from the Authorized signatory of the CSP on their letterhead.
5	Proposed CSP shall have an average turnover from cloud services in India of Rs. 2000 Crore in the last three (3) financial years i.e. (2019-20, 2020-21 and 2021-22).	Audited Balance Sheets and Profit & Loss account for the last three financial years and certificate from the statutory auditor shall be submitted. If the turnover is from fields other than IT services, then certificate from statutory auditor to be submitted for turnover from IT services separately (Supported with Form A6 certified by statutory auditor).
6	Proposed CSP should be certified for ISO 27001, ISO 27017 and ISO 27018, ISO 22301, 27701:2019	Copy of Valid Certificates
7	Proposed Cloud Solution to be deployed across different physical locations, with active-active configuration to ensure fault tolerance with high availability between two physical sites.	Self-certificate from the Authorized signatory of the CSP on their letterhead.
8	CSP should have minimum 3 Nos. of MeitY empaneled and STQC audited data centers in physically different locations in India.	Self-certificate from the authorized signatory of the CSP on their letterhead confirming that they have 3 data centers in India. The same should be confirmed from the MeitY website as well.
9	CSP should be in continuous business of the Hosting and Maintenance of Cloud infrastructure in India for more than **Five (5)** years prior to the bid opening.	Self-Certificate from the Authorized signatory of the CSP on their letterhead.

10	CSP should have SAP-certified instances for running SAP HANA DB. Information about the instance types that are certified and supported for SAP should be available in public domain reference link	Self-Declaration from the Authorized signatory of the CSP on their letterhead.& Public Referenceable link
11	CSP should offer multiple pricing models such as Pay-As-You-Go, Reserved and other such models for helping optimization of cost.	Self-certified letter from CSP on their letterhead.
12	CSP should have published on its public facing website about cloud services' rates for India, Service Level Agreements (SLAs), dashboard live-status of cloud services' health across global datacenter and outage details (if any) with RCA	Self-certified letter from CSP on their letterhead.

4. COST OF BIDDING

4.1 The Bidder shall bear all costs associated with the preparation and submission of its bid, and HLL, will in no case be responsible or liable for these costs, regardless of the conduct or outcome of the bidding process.

4.2 Tender documents may be downloaded free of cost from the Government e-procurement portal (URL: https://etenders.gov.in/eprocure/app). However, tender document fees, as mentioned in the NIT, is required to be submitted along with the online bid.

5. Getting information from web portal

5.1. All prospective bidders are expected to see all information regarding submission of bid for the Work published in the e tender website during the period from the date of publication of NIT for the Work and up to the last date and time for submission of bid. Non observance of information published in the website shall not be entertained as a reason for any claim or dispute regarding a tender at any stage.

5.2. All bids shall be submitted online on the Government e-procurement portal only in the relevant envelope(s)/ cover(s), as per the type of tender. No manual submission of bids shall be entertained for the tenders published through Government e-procurement portal under any circumstances.

5.3. The Government e-procurement portal shall not allow submission of bids online after the stipulated date & time. The bidder is advised to submit the bids well before the stipulated date & time to avoid any kind of network issues, traffic congestion, etc. In this regard, the department shall not be responsible for any kind of such issues faced by bidder.

6. Bidding Documents

6.1. Content of Bidding Documents

6.1.1. The bidding documents shall consist of the following unless otherwise specified

a. Notice Inviting Tender (NIT)
b. Introduction
c. General Instructions to Bidders
d. General Conditions of Contract
e. Scope of work
f. Form and Annexures

6.1.2. The Bidder is required to login to the e-procurement portal and download the listed documents from the website as mentioned in NIT. He shall save it in his system and undertake the necessary preparatory work off-line and upload the completed bid at his convenience before the closing date and time of submission.

6.1.3. The bidder is expected to examine carefully all instructions, Conditions of Contract, Contract Data, Terms, Technical and functional Specifications, Forms & Annexures in the Bid Document. Failure to comply with the requirements of Bid Document shall be at the Bidder’s own risk.

6.2 Clarification of Bidding Documents

6.2.1. A prospective bidder requiring any clarification of the bidding documents shall contact the office of the Tender Inviting Authority on any working day between 10 AM and 5 PM.

6.2.2. In case the clarification sought necessitates modification of the bid documents, being unavoidable, the Tender Inviting Authority may affect the required modification and publish them in the Government e procurement portal through corrigendum.

6.3 Amendment to bidding documents

6.3.1. Before the deadline for submission of bids, the Tender Inviting Authority may modify the bidding document by issuing addenda.

6.3.2. Any addendum thus issued shall be a part of the bidding documents which will be published in the Government e procurement portal. The Tender Inviting Authority will not be responsible for the prospective bidders not viewing the website in time.

6.3.3. If the addendum thus published does involve major changes in the scope of work, the Tender Inviting Authority may at his own discretion, extend the deadline for submission of bids for a suitable period to enable prospective bidders to take reasonable time for bid preparation taking into account the addendum published.

7. Preparation of Bids

7.1 Language of the Bid

7.1.1. All documents relating to the bid shall be in the English language.

7.2. Documents Comprising the Bid

7.2.1. The online bid submitted by the bidder shall comprise the following:

1. Details required for e-payment (Details of bank account having core banking facility and e-mail address of the bidder) in the prescribed format.
2. Payment of bid submission/tender fee as detailed in the e-tender web site.
3. Bid Security (EMD) payment details.
4. Copy of Registration (GST, PAN etc.) Certificate duly attested.
5. Copy of Documents in proof of eligibility criteria

6. Copy of Documents in proof of financial turnover.
7. Other documents specified in tender.
8. Priced Bid.

7.2.2. Bidders shall not make any addition, deletion or correction in any of the bid documents. If tampering of documents is noticed during tender evaluation, the bid will be rejected and the bidder will be blacklisted.

7.3. Bid Prices

7.3.1. The Bidder shall bid for the whole work as described in the scope of work.

7.3.2. For item rate tenders, the bidder shall fill in rates in figures and should not leave any cell blank. The line item total in words and the total amount shall be calculated by the system and shall be visible to the Bidder.

7.3.3. The rates quoted by the Bidder shall include cost of all services, Labour charges, overheads and all incidental charges for execution of the contract. The rate quoted shall also include all statutory taxes as on the date of submission of the tender and such taxes shall be paid by the contractor.

7.3.4. GST or any other tax applicable shall be payable by the Contractor in respect of this contract and HLL will not entertain any claim whatsoever in respect of the same.

7.3.5. All taxes, royalty, Octroi and other levies payable by the bidder under the contract, or for any other cause as of the date 28 days prior to the deadline for submission of bids shall be included in the rates, prices and total of bid price. The bid prices shall also cater for any change in tax pattern during the tenure of work.

7.3.6. The rates and prices quoted by the bidder shall remain firm during the entire period of contract.

7.4. Currencies of Bid and Payment

7.4.1. The currency of bid and payment shall be quoted by the bidder entirely in Indian Rupees. All payments shall be made in Indian Rupees only.

7.5. Bid Validity

7.5.1. Bids shall remain valid for the period of **180 (One Hundred and Eighty)** days from the date of opening of the bid as specified in the NIT. A bid valid for a shorter period shall be rejected by HLL as Non Responsive.

7.5.2. In exceptional circumstances, prior to expiry of the original bid validity period, the Tendering Authority may request the bidders to extend the period of validity for a specified additional period. The request and the responses thereto shall be made in writing or by e mail. A bidder may refuse the request without forfeiting its bid security. Extension of validity period by the Bidder must be unconditional. A bidder agreeing to the request will not be required or permitted to modify its bid, but will be required to extend the validity of its bid security for the period of the extension.

7.6. Bid Security Declaration

7.6.1. In case of MSE or Start-up who are eligible for EMD exemption should provide a Bid Security Declaration is to be attached in the format (Form-A9) given in the tender.

7.6.2. In case of MSE or Start-up who are eligible for EMD exemption, any Bid not accompanied by Bid Security Declaration shall be rejected as non-responsive.

7.7. Bid submission fee

7.7.1. For e-tenders, the mode of remittance of Bid submission fee (Tender Fee) shall be the same as detailed for remitting Bid Security. For e-tenders, Bidders shall remit the Tender fee using the payment options as mentioned in the e-tender in Government e-Procurement portal only.

7.7.2. Any bid not accompanied by the Tender Fee as notified, shall be rejected as non-responsive.

7.7.3. Tender Fee remitted will not be refunded.

7.8 Alterations and additions

7.8.1. The bid shall contain no alterations or additions, except those to comply with instructions, or as necessary to correct errors made by the bidder, in which case such corrections shall be initiated by the person or persons signing the bid.

7.8.2. The bidder shall not attach any conditions of his own to the Bid. The Bid price must be based on the tender documents. Any bidder who fails to comply with this clause will be disqualified.

8. Submission of Bids

The Bidder shall submit their bid online only through the Government eProcurement portal (URL: https://etenders.gov.in/eprocure/app) as per the procedure laid down for e-submission as detailed in the web site. For e tenders, the bidders shall download the tender documents from the portal. The Bidder shall fill up the documents and submit the same online using their Digital Signature Certificate. On successful submission of bids, a system generated receipt can be downloaded by the bidder for future reference. Copies of all certificates and documents shall be uploaded while submitting the tender online.

8.1 The tender is invited in **3 Envelope system** from the registered and eligible firms at CPP Portal.

8.2 Pre-qualification Criteria for bidders: Following 3 envelopes shall be submitted online at CPP-portal by the bidder.

a) **Envelope - I (Tender Fee and EMD):**

Tender fee (Non-refundable) and EMD as per the tender conditions shall be paid separately, thru RTGS/NEFT transfer in the following HLL A/c details:

Name of Bank	:	State Bank of India
A/c number	:	10183256222
IFSC Code	:	SBIN0004350
Branch name	:	Commercial Branch, Thiruvananthapuram

Document of the above transactions completed successfully by the bidder, shall be uploaded separately while submitting the bids online.

Note:-

SSI/MSME units interested in availing exemption from payment of Tender Fee and EMD should submit a valid copy of their registration certificate issued by the concerned DIC or NSIC/Udyog Aadhar. If the bidder is a MSME, it shall declare in the bid document the Udyog Aadhar Memorandum Number issued to it under the MSMED Act, 2006. If a MSME bidder do not furnish the UAM Number along with bid documents, such MSME unit will not be eligible for the benefits available under Public Procurement Policy for MSEs Order 2012. But the Party has to provide Performance Security/Security Deposit if Tender is awarded to them.

b) **Envelope -II (Technical bid): documents mentioned in the eligibility criteria table**

Technical Bid should contain

- Copy of valid Certificate of Incorporation or Certified copy of valid Partnership Deed.
- Self-attested copy of PAN card under Income Tax Act
- Self-attested copy of GST Registration Number and details
- Valid copy of MSME/NSIC Registration Certificate along with the list of items / services for which they are registered, as issued by NSIC for EMD exception, if applicable.
- Documents to prove the Eligibility Criteria as mentioned in Clause 3.1 & 3.2 of this document.
- Project approach plan and methodology
- Original tender document duly signed and sealed on all pages (including scope of work, general Terms & Conditions and Annexure).
- Pre-qualification criteria compliance checklist as given in Form A1 of this document
- Details of the Bidder (on Letterhead) as given in Form A2 of this document
- Financial Capability Report as given in Form A3 of this document
- Letter of Confirmation / Declaration as given in Form A4 of this document

- Compliance Checklist as given in Form A5 of this document
- Technical Compliance Statement as given in Form A6 of this document
- Any other relevant documents if enclosing by the bidder.

c) **Envelope – III (Financial Bid): The Financial e-Bid through CPP portal.**

All rates shall be quoted in the format provided and no other format is acceptable. If the price bid has been given as a standard format with the tender document, then the same is to be downloaded and to be filled by all the bidders. Bidders are required to download the file, open it and complete all the cells with their respective financial quotes and other details (such as name of the bidder, CSP and other details), without omission. No other cells should be changed. Once the details have been completed, the bidder should save it and submit it online, without changing the file-name. If the file is found to be modified by the bidder, the bid will be rejected. The pdf format of the price bid also needs to be attached.

Note:-

1. HLL Lifecare Limited reserves the right to verify the credential submitted by the bidder at any stage (before or after the award the work). If at any stage, any information / documents submitted by the bidder is found to be incorrect / false or have some discrepancy which disqualifies the firm then HLL shall take the following action:

   a) Forfeit the entire amount of EMD submitted by the firm.

   b) The bidder shall be liable for debarment from tendering in HLL Lifecare Limited, apart from any other appropriate contractual /legal action.

   On demand of the Tender Inviting Authority, this whole set of certificates and documents shall be sent to the Tender Inviting Authority's office address (as given in the NIT) by registered post/Speed post of India Post in such a way that it shall be delivered to the Tender Inviting Authority before the deadline mentioned. The Tender Inviting Authority reserves the right to reject any bid, for which the above details are not received before the deadline.

2. The Tender Inviting Authority shall not be responsible for any failure, malfunction or breakdown of the electronic system while downloading or uploading the documents by the Bidder during the e-procurement process.

9. Deadline for Submission of the Bids

9.1 Bid shall be received only online on or before the date and time as notified in NIT.

The Tender Inviting Authority, in exceptional circumstances and at its own discretion, may extend the last date for submission of bids, in which case all rights and obligations previously subject to the original date will then be subject to the new date of submission. The Bidder will not be able to submit his bid after expiry of the date and time of submission of bid (server time).

9.2 Modification, Re-submission and Withdrawal of Bids

9.2.1 Re-submission or modification of bid by the bidders for any number of times before the date and time of submission is allowed. Re-submission of bid shall require uploading of all documents including price bid afresh.

9.2.2 If the bidder fails to submit his modified bids within the pre-defined time of receipt, the system shall consider only the last bid submitted.

9.2.3 The Bidder can withdraw his/her bid before the date and time of receipt of the bid. The system shall not allow any withdrawal after the date and time of submission.

10. Contract Period and Commercials

10.1 The contract period of the services will be **Three (3) years** only from the date of commissioning of the proposed Cloud infrastructure as mentioned in the BOQ (Annexure1) subject to the verification by HLL. However HLL reserves the right to extend/renew the contract period at its discretion.

10.2 If the services are found not satisfactory, Purchaser reserves the right to terminate the services by giving one month notice period.

10.3 The BOQ quantities are indicative and estimated for the evaluation purpose only. No commitment shall be made for the execution of these quantities.

10.4 During the execution of the contract, the actual consumption of the services may change.

10.5 Payment will be done as per the actual quantities utilized during the execution of the contract

10.6 In the event of any additional services is required outside the BOQ, the MSP is liable to provide such services with the discounted rate from the public listed Price of the CSP throughout the entire contract period of 3 years.

11. TIME SCHEDULE

Sl No	Activity	Description	Time Duration
1	Acceptance of Work Order	Date of Receipt of signed Work Order	Within 7 Days from The date of Work Order
2	Service Delivery of the Proposed Cloud Environment	Provisioning of cloud services like account setup, cloud security services, user roles & permissions etc., storage services and network connectivity	Within 28 Days from the date of Work Order
3	Operational Acceptance	Satisfactory Configuration of Cloud Environment after fine tuning of Performance and Testing of Connectivity	Within 42 Days from the Date of Work Order
4	SLA	Date of Signed Agreement	Within 10 days from the Date of Operational acceptance
5	Operation and Maintenance phase	Continuous Monitoring and Maintenance of the configured Cloud infrastructure	3 years from the date of operational acceptance.

12. Bid Opening and Evaluation

12.1. Bid Opening

Bids shall be opened on the specified date & time, by the tender inviting authority or his authorized representative in the presence of bidders or their designated representatives who choose to attend.

12.1.1 Bid Opening Process

12.1.2. Opening of bids shall be carried out in the same order as it is occurring in invitation of bids or as in order of receipt of bids in the portal. The bidders & guest users can view the summary of opening of bids from any system. Bidders are not required to be present during the bid opening at the opening location if they so desire.

a) Envelope - I: Envelope - I Opening date shall be mentioned in NIT Document. (Envelop – I shall contain scanned copy of Tender Fees and EMD)

b) Envelope - II: Envelop - II opening date shall be as mentioned in NIT Document. The intimation regarding acceptance/rejection of their bids will be intimated to the contractors/firms through e-tendering portal. (Envelope-II shall contain scanned copy of Pre-qualification document.)

   If any clarification is needed from bidder about the deficiency in his uploaded documents in Envelope-I and Envelope-II, he will be asked to provide it through CPP portal. The bidder shall upload the requisite clarification/documents within time specified by HLL Lifecare Limited, failing which tender will be liable for rejection.

c) Envelope - III: The financial bids of the bidders found to be meeting the qualifying requirements shall be opened as per NIT Document. (Depending on evaluation of Envelop I & II, the date shall be intimated through CPP Portal)

12.1.3. In the event of the specified date of bid opening being declared a holiday for HLL, the bids will be opened at the same time on the next working day.

12.2. Confidentiality

12.2.1. Information relating to the examination, clarification, evaluation, and comparison of Bids and recommendations for the award of a contract shall not be disclosed to Bidders or any other persons not officially concerned with such process until the award has been announced in favour of the successful bidder.

12.2.2. Any effort by a Bidder to influence the Purchaser during processing of bids, evaluation, bid comparison or award decisions shall be treated as Corrupt & Fraudulent Practices and may result in the rejection of the Bidders' bid.

12.3. Clarification of Bids

12.3.1. To assist in the examination, evaluation, and comparison of bids, the Tender Inviting Authority may ask the bidder for required clarification on the information submitted with the bid. The request for clarification and the response shall be in writing or by e-mail, but no change in the price or substance of the Bid shall be sought, offered, or permitted.

12.3.2. No Bidder shall contact the Tender Inviting Authority on any matter relating to the submitted bid from the time of the bid opening to the time the contract is awarded. If the Bidder wishes to bring additional information to the notice of the Tender Inviting Authority, he shall do so in writing.

12.4. Examination of Bids and Determination of Responsiveness

12.4.1. During the bid opening, the Tender Inviting Authority will determine for each Bid whether it meets the required eligibility as specified in the NIT; is accompanied by the required bid security, bid submission fee and the required documents and certificates.

12.4.2. If a Bid is not substantially responsive, it may be rejected by the Tender Inviting Authority, and may not subsequently be made responsive by correction or withdrawal of the nonconforming material deviation or reservation.

12.4.3. Non submission of legible or required documents or evidences may render the bid non-responsive.

12.4.4. Single tender shall not be opened in the first tender call.

12.5. Evaluation Criteria for Technical Bid & Commercial Bid

The evaluation of bids shall be done in 3 stages:

STAGE-I: Response to Mandatory Requirements.

The evaluation committee, appointed by the HLL as a whole, evaluates the proposals on the basis of their responsiveness to the Eligibility Criteria as mentioned in Clause 3.1 & 3.2 of this document. Proposal shall be rejected at this stage if it does not respond to Eligibility Criteria. The Eligibility Criteria are to be met by the Bidder for the proposed work (Installation, Configuration and Maintenance of Cloud Based Infrastructure for hosting the SAP Applications of HLL).

Only those bidders who meet all the Eligibility Criteria as provided in **Clause 3.1 & 3.2** in this document shall be considered for Stage II evaluation.

STAGE-II: Evaluation of Technical Bid

The evaluation committee, appointed by the HLL, evaluates the proposals on the basis of their responsiveness to the Scope of Work (SoW) as mentioned in **Part IV and** Technical Compliance Statement as given in Form A6 in this document. Each responsive proposal will be given a technical score. A proposal shall be rejected at this stage if it fails to achieve the minimum Technical Score (**80 Marks**) as indicated below:

- Calculating score (**St**) for Technical Requirements of the Solution:
    - ➢ Responses as provided by bidders would be evaluated using following Evaluation Criteria;

Sl. No	Value	Rating Criteria	Max Marks	Documentary Evidence
A	**CSP Cloud Rating Matrix**			
1	Average Annual Turnover of CSP	The proposed CSP shall have annual turnover from provisioning cloud services in India in last financial year (2021-2022) Rating Criteria : 2,000 to 4,000 Cr. = 3 marks > 4000 Cr. = 5 marks	5	Certificate from Chartered Accountant on their letterhead mentioning the annual revenue from Provisioning Cloud Services in India
2	CSP Experience – SAP workloads	Proposed CSP shall have experience of hosting SAP Applications. Rating Criteria : • Active Customers > 2000 - 5 Marks • 1000 to 2000Active Customers – 2 Marks	5	Self-declaration from the Authorized signatory of the CSP on their letterhead with Public Reference link.
3	CSP Experience – SAP workloads	Minimum 3 SAP migration case studies/referenceable customers in India should have happened on the proposed CSP platform. • Customer experience with minimum 3workloads – 2 marks • Customer with more than or equal to 5 workloads – 5 Marks	5	Self-certificate from CSP with customer contact details

Sl. No	Value	Rating Criteria	Max Marks	Documentary Evidence
4	SAP certified instances	CSP should have more than 100+ instances certified by SAP. Information about the instance types that are certified and supported for SAP should be available in public domain reference link.	5	Undertaking on CSP letterhead with link to SAP public facing website
5	Cloud Availability & SLA	CSP should have available SLA of >= 99.95% (calculated monthly) for the compute and block storage services offered as per the published SLAs of the CSP; • SLA >= 99.99% - 5 marks SLA >= 99.95% - 2 marks	5	Undertaking on CSP letterhead with link to public facing website having the service and functionality description
6	Cloud services availability	The Proposed CSP compute services should offer at least 3 different processor architecture support as Intel x86, AMD & ARM based computer services from India Region.	5	Undertaking on CSP letterhead with link to public facing website
7	Cloud PaaS	Availability of relevant native PaaS services from the CSP for the current requirement**:** 1. Machine Learning service: 1 mark 2. Server less computing platform: 1 mark 3. Managed ETL service: 1 mark 4. Managed Server less Analytics service: 1 mark	10	Undertaking on CSP letterhead with link to public facing website having the service and functionality description

Sl. No	Value	Rating Criteria	Max Marks	Documentary Evidence
		5. Managed Data warehousing / Data Lake: 1 mark 6. Infrastructure provisioning and Automation: 1 mark 7. IoT service: 1 mark 8. Security –DDoS protection: 1 mark 9. Security – Threat detection service: 1mark 10. Cloud Native Bulk Email service (for transactional emails, etc.): 1 mark		
8	Cloud Storage	CSP shall offer Different tier of Managed Object storage service; 1. Storage Class: class/tier that automatically migrates data between classes/tiers : 2 mark 2. Storage Class: class/tier with automatic in-region replication to 2 or more Availability Zones : 3 mark	5	Undertaking on CSP letterhead with link to public facing website having the service and functionality description
9	Databases	CSP must have their own native service Availability of managed databases (PAAS) having feature of inbuilt scaling, HA & backup for following Databases i. MySQL : 1 mark ii. PostgreSQL : 1 mark iii. Maria DB : 1 mark iv. MS SQL Server : 1 mark v. Oracle : 1 mark	5	Undertaking on CSP letterhead with link to public facing website having the service and functionality description

Sl. No	Value	Rating Criteria	Max Marks	Documentary Evidence
10	Cloud Services Architecture	Proposed CSP Architecture is required to be a multi-site deployment, across geographically disparate MeitY empaneled sites, with Active-Active configuration to ensure fault-tolerance with high availability between two physical sites and automated processes to shift application traffic to a secondary physical site	10	Undertaking on CSP letterhead with link to public facing website having the service and functionality description
11	Industry Analyst Reports	Presence of CSP as Leader in the Gartner's Magic Quadrant of Cloud Infrastructure as a service worldwide; Present: 5 Marks	5	Undertaking on CSP letterhead with valid Gartner's Report
12	* Technical presentation – covering the profile of MSP and their technical capability to manage the work	Presentation by MSP based on their Technical Proposal with overall project plan and solution architecture in compliance with Scope of work given in the tender.	15	Presentation in front of HLL Technical committee
13	* Technical presentation – covering the CSP capabilities.	Demo covering CSP Platform capabilities as mentioned in the Table A	15	Presentation in front of HLL Technical committee

Sl. No	Value	Rating Criteria	Max Marks	Documentary Evidence
14	Technical Specifications	Complete compliance to Technical specifications – 5 marks	5	Technical compliance matrix as given in Form A6
TOTAL (St)			100	

*__Details of the Technical presentation are as follows__;

- Bidders and associated CSP are required to give a presentation before HLL Technical Committee on methodology proposed for the work mentioned in this tender.

- Presentation is for demonstrating the ability of the bidder to effectively deliver Managed Services and the associated CSP to deliver prompt services as mentioned under Part IV (Scope of Work)

- Presentation will be scheduled by HLL and intimated to the eligible responsive bidders after STAGE-I Evaluation (Response to Mandatory Requirements).

- Each bidder will get a total of 30 Minutes for both MSP and CSP Presentation followed by clarification if any from HLL.

- Marks awarded by the earmarked Technical Committee of HLL for the presentation will be final and binding.

- Deliverables as committed by the bidder and the associated CSP in presentation shall be considered as part of the contract.

Demo requirements - Table A

Sl. No	Requirements	Functionality which needs to be demonstrated
1	CSP should have capability to provide insights about the access, usage etc. with a dashboard.	Login to the cloud console, create object storage with read permission and change permission for object storage to write from read, and then check in the dashboard and check insights on user access and changes.
2	System should be able to provide ability to automatically increase / scale the number of Instances/VMs during demand spikes for few hours /days to maintain performance	Auto scaling capability as per defined parameters like CPU utilization, number of requests, RAM utilization etc. Evaluate on ability to auto-scale; ease of configuring the auto-scaling rules, breadth of parameters for configuring auto-scaling (e.g., min/max/parameters on which threshold levels can be set/wait time), availability of multiple auto-scaling scenarios (e.g., based on threshold levels, scheduled, recurring).
3	No prior intimation or buffer will be given, as increase/decrease number of instances should happen automatically based on the controls/parameters set up for maximum/minimum usage of VMs.	Functionality as described in the clause
4	System should be able to provide metering and billing of services like VMs, storage, Managed Databases including MySQL, Postgres licenses at **hourly granularity**.	Complete demo of managed database with high availability (instance failover), synchronous replication to different physical datacenter, backup, restore and snapshot.

5	CSP should have the ability to auto-scale without human intervention; ease of configuring the auto-scaling rules, parameters for configuring auto-scaling (e.g., min/max/parameters on which threshold levels can be set/wait time), availability of multiple auto-scaling scenarios (e.g., based on threshold levels, scheduled, recurring).	Functionality as described in the clause
6	Capability to create policies that can restrict access to the data based on user.	Functionality as described in the clause
7	Support server-side encryption (SSE) of data "at-rest", with the cloud provider managing the encryption keys or customer provided cryptographic keys	Functionality as described in the clause
8	Support read-after-write consistency for addition of any object (PUT operations)	Functionality as described in the clause

- The HLL shall notify the bidders that have secured the minimum qualifying mark (80 Marks), indicating the date and time set for opening the Financial Proposals.

STAGE-III: Evaluation of Price Bid

The Financial Proposals shall be opened publicly in the presence of the representatives of the bidders who choose to attend. The evaluation committee will determine whether the Financial Proposals are complete (i.e., whether all items of the corresponding Technical Proposals and as per the BOQ (Annexure-1) have been costed). The bidders, who confirm all the commercial conditions and submitted the required documents as per the tender are considered as commercially acceptable. The financial proposal quoted with partial items will be summarily rejected.

- Total Cost of Ownership (TCO) will be calculated by adding the following elements as listed in BOQ (Annexure-1) of prices.
- The Bid having the Lowest TCO shall be termed as the Lowest Evaluated Bid and will be awarded **30 Marks**.

- Financial score (Sf) of other bidders will be calculated on the basis of the following formula:

$$\mathbf{Sf = 100 \times Fm / F}$$

Where Sf is the financial score, Fm is the lowest price among all bidders and F the price of the proposal of the respective bidder under consideration.

STAGE-IV: Final Evaluation of Bidders

Final Evaluation of the qualified bidders in **STAGE II (Evaluation of Technical Bids)** will be done as follows;

- Proposals will be ranked according to their combined technical (St) and financial (Sf) scores using the weights (T = the weight given to the Technical Proposal; P = the weight given to the Financial Proposal; T + P = 1).

The weights given to the technical and Financial Proposals are:

T= 0.70

P= 0.30

Total score of the bidding party will be determined based on the following formula:

$$\mathbf{S = (St \times T) + (Sf \times P)}$$

The bidder achieving the **highest total score** will be considered for placement of order.

12.6 Technical Presentation

12.6.1 Bidders and associated CSP are required to give a presentation before HLL Technical Committee on methodology proposed for the work mentioned in this tender.

12.6.2 Presentation is a part of the Technical Evaluation Criteria with marks allotted to it alongside other evaluation criteria as mentioned in STAGE II Evaluation (Evaluation of Technical Bids) under Clause 12.5 of this document.

12.6.3 Presentation is for demonstrating the ability of the bidder to effectively deliver Managed Services and the associated CSP to deliver prompt services as mentioned under Part IV (Scope of Work)

12.6.4 Presentation will be scheduled by HLL and intimated to the eligible responsive bidders after STAGE-I Evaluation (Response to Mandatory Requirements) under Clause 12.5 of this document.

12.6.5 Each bidder will get a total of 30 Minutes for both MSP and CSP Presentation followed by clarification if any from HLL.

12.6.6 Marks awarded by the earmarked Technical Committee of HLL for the presentation will be final and binding.

12.6.7 Deliverables as committed by the bidder and the associated CSP in presentation shall be considered as part of the contract.

13. Award of Contract

13.1. HLL will award the Contract to the Bidder who score Highest Marks in the Evaluation Criteria.

13.2. In the eventuality of failure on the part of the bidder who score highest marks to accept the Letter of acceptance (LOA) / Work Order within the specified time limit, the Bidder's EMD shall be forfeited

13.3 The rates for the various items quoted by the Bidder shall be rounded to two decimal places. The decimal places in excess of two will be discarded during evaluation.

13.4 HLL reserves the right to accept or reject any Bid and to cancel the Bidding process and reject all Bids at any time prior to the 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 the Tender Inviting Authority's action.

13.5 Before awarding the contract, HLL reserves the right to negotiate with the bidder who scores highest score in the evaluation of bids.

14. Corrupt or Fraudulent Practices

14.1 The purchaser requires that the bidders, suppliers and contractors observe the highest standard of ethics during the procurement and execution of such contracts. In pursuit of this policy, the following are defined:

Sl. No.	Term	Meaning
(a)	Corrupt practice	The offering, giving, receiving, or soliciting, directly or indirectly, of anything of value to influence the action of a public official in the procurement process or in contract execution.
(b)	Fraudulent practice	A misrepresentation or omission of facts in order to influence a procurement process or the execution of a contract.
(c)	Collusive practice	Means a scheme or arrangement between two or more bidders, with or without the knowledge of the purchaser, designed to establish bid prices at artificial, non-competitive levels.
(d)	Coercive practice	Means harming or threatening to harm, directly or indirectly, persons or their property to influence their participation in the procurement process or affect the execution of a contract.

14.2 The Purchaser will reject a proposal for award if it determines that the Bidder recommended for award has, directly or through an agent, engaged in corrupt, fraudulent, collusive or coercive practices in competing for the Contract in question.

15. Price

Price quoted should be firm without any escalation till the order is completely executed. The price quoted should be inclusive of all material cost, license charges if any , all applicable taxes (except GST) and other levies, Labour charges, insurance, Installation and commissioning charges and whatsoever expenses / charges applicable for the successful completion of the contract etc.

16. Taxes/Duties/Levies

The bidder shall be entirely responsible for all applicable taxes including GST, duties, license fees if any etc. incurred until successful completion of contract. Any change in GST upward/downward as a result of any statutory variation (from the date of opening of price bid till the last date of completion of work without applicability of LD) in GST taking place within contract terms shall be allowed to the extent of actual quantum of GST paid by the MSP. In case of downward revision in

GST, the actual quantum of reduction of GST shall be reimbursed to HLL by the MSP. All such adjustments shall include all reliefs, exemptions, rebates, concession etc. if any obtained by the supplier.

17. Completion Time

The proposed Cloud infrastructure is to be ready for hosting SAP Applications as per the mutually finalized project plan from the date of formal kick-off meeting in not more than 6 weeks from the release of PO/LOA

18. EMD

Earnest Money Deposit (EMD) of Rs.6, 00,000/- (Rupees Six Lakh Only) shall be remitted through an e-payment in favour of HLL Lifecare Limited.

- No interest will be payable to EMD. EMD's of unsuccessful bidders will be returned only after awarding the work to the successful bidder.
- The EMD of the successful bidder will be returned only after execution of the Contract Agreement and after furnishing of the required Security Deposit / Performance Bank Guarantee.
- Bidders with valid registration under National Small Industrial Corporation (NSIC) / Micro Small and Medium Enterprises (MSME) will be eligible for all relaxation subject to the submission of valid documents. To qualify for EMD exemption, firms should necessarily submit valid copy of the Registration Certificate along with the list of items / services for which they are registered, as issued by NSIC, in Part-I Technical Bid.
- Request for exemption from EMD other than from the eligible MSE's and Start-up's will not be entertained.

The EMD security may be forfeited:

1. If a Bidder withdraws its bids during the period of bid validity
2. If a Bidder makes any statement or encloses any form which turns out to be false/incorrect at any time prior to signing of the contract
3. In case of successful Bidder, if the Bidder fails to Sign the contract.

19. Performance Bank Guarantee

19.1 The successful bidder shall furnish a Performance Bank Guarantee (PBG) or Performance Security Deposit (DD, NEFT) for an amount equivalent to 3% of the contract value within 14 days of the receipt of LOA/PO. Failure to submit PBG or Security deposit within 14 (Fourteen) days from the LOA / PO, will lead to the cancellation of contract.

19.2 The Performance Bank Guarantee (PBG) shall be as per the format given in Annexure 3 of this document valid till the completion of the contract plus a claim period of 60 days from a Nationalized Indian Bank/Scheduled bank, payable at a designated bank branch located in Thiruvananthapuram.

19.3 The expenses to be incurred for the making of Performance Bank Guarantee (PBG) shall be borne by the Contractor.

19.4 Renewal of Performance Security Deposit: In case the contract period is likely to be delayed, HLL will instruct the bidder to extend the validity of security deposit till the completion of contract period. In case, Bank Guarantee for security deposit is not extended/ renewed by the bidder as per the request of HLL, HLL may withhold the equivalent amount from the immediate next payment due for the bidder.

19.5 The Purchaser shall be entitled on his part to forfeit the amount of the Performance Bank Guarantee/Security deposit in whole or in part in the event of any default, failure or neglect on the part of the Contract in the fulfillment or performance in all respects of the contract.

19.6 Refund of Performance Security Deposit: Security Deposit will be refunded to the bidder without any interest, within 60 days after the bidder has duly performed and completed the contract in all respects.

20. Payment terms

SI No.	Milestone for Payment	Payment Schedule
1.	Monthly Invoice generated against CSP cost based on actual usage	Monthly
2.	Monthly Invoice for the Managed Services if any.	Monthly
2.	One Time Implementation Cost if any	One Time (After successful Implementation of Cloud Infrastructure)

- Payment will be made by RTGS / NEFT to the account of MSP. The name of the bank, branch, A/C No., IFSC code & other particulars shall be furnished by the MSP in the pro- forma of HLL.
- The unit cost of all services listed in BoM shall be quoted in INR. In case CSP list price is available in USD only then for bid purposes exchange rate of 1 USD = INR on bid submission date shall be used.
- In case "quoted unit price for a service" and "public listed price of the service" is different, lower of the two shall be applicable.
- HLL may use any service from offerings of CSP on Pay as you Go basis and the payments shall be made based on actual consumption. The bidder must specify the discount offered on publicly available list price of CSP pay-as-go services and same shall be applied on services used but not listed in BOM.
- In case, MSP has declared the list price of CSP to be in USD, the exchange rate on last of the month (as per RBI) shall be considered for that particular month invoice.
- All payments will be made on monthly basis and in INR only.

21. Pre-bid Queries

a. All bidders are advised to study the bid document thoroughly before raising any clarifications/queries.

b. Any bidder requiring a clarification of the bid document must notify HLL by email **on or before 15.02.2023, 17.00 Hrs** in the pre-bid questionnaire format

(Form-A8) given in this document. Any request for clarification must be addressed to **erp@lifecarehll.com**.

c. The compilation of all clarifications sought / queries and its replies shall be made available as corrigendum in Central Public Procurement Portal (CPP). Any modification of the RFP which may become necessary as a result of the pre-bid queries shall be made by HLL exclusively through the issuance of corrigendum.
d. It may be noted that no queries of any bidder shall be entertained after the deadline for submitting the queries.

22. Indemnification Clause

The bidder shall indemnify and hold harmless the Purchaser from and against all claims, liability, loss damage or expense, including counsel fees arising from or by reason of any actual or claimed trade mark, patent or copy right infringement or any litigation based thereon with respect to any part of the items covered by the Contract, and such obligations shall survive acceptance of payment for the items.

23. Confidentiality

This request for proposal and all materials submitted by HLL for this purpose, must be considered confidential, and may not be distributed or used for any purpose other than the preparation of a response for submission to HLL.

The Bid documents shall remain the exclusive property of the HLL without any right to the Bidder to use them for any purpose other than the preparation of a response for submission to HLL. Non-disclosure agreement (NDA) as per Annexure- 2 of this document shall be signed by the successful bidder. Disclosure of any part of the information contained therein to parties not directly involved in providing the services /products requested, could result in disqualification and/or legal action. When submitting confidential material to HLL, the bidder must clearly mark it as such.

24. Conflict of Interest

HLL requires that bidder strictly avoid conflicts with other assignments/jobs or their own corporate interests and act without any consideration during the System

Integration services. In case the bidder has any subsisting interest, either by themselves or through their partners, that is likely to conflict the work specified in the Scope of Work, HLL reserves the right to accept or reject such bids.

25. Risk Purchase

If the supplier fails to provide the service/ project phase ordered within the delivery period as per Project plan or violate any of the terms and conditions of the contract, HLL shall have right to terminate the contract with 15 days' notice forfeiting the EMD.

26.Liquidated Damage for Delays

If the bidder fails in the due performance of the contract within the time fixed by the contract or any extension thereof, bidder shall be liable to pay liquidated damages to the extent of a sum of 0.5% of the contract value per week subject to a maximum of 5 % of the contract value excluding tax. Once the maximum is reached, HLL may consider termination of the contract. In assessing such delays, HLL Project Manager's decision is final.

27. Jurisdiction

All questions, disputes or difference arising under, out of, or in connection with contracts shall be subject to the exclusive jurisdiction of the Courts at Thiruvananthapuram, Kerala, India.

28. Force Majeure

In the event of either party being rendered unable by `Force Majeure' to perform any obligation required to be performed by them under the contract, the relative obligation of the party affected by such `Force Majeure' will stand suspended for the period during which such cause lasts. The word `Force Majeure' as employed herein shall mean acts of God, war, revolt, agitation, strikes, riot, fire, flood, sabotage, civil commotion, pandemic, acts of government of the two parties, which makes performance impossible or impracticable and any other cause, whether of kind herein enumerated or otherwise which are not within the control of the party to the contract and which renders performance of the contract by the said party impossible. HLL may allow additional time as is mutually agreed, to be justified by the circumstances of the case. The occurrence/ cessation of force majeure situation is to be informed with documentary evidence within 15 days from the date of occurrence/cessation.

29. Termination of the Process

HLL may terminate the bidding process at any time without assigning any reason. HLL makes no commitments, express or implied, that this process will result in a business transaction with anyone.

The contract with the successful bidder may be terminated in the following circumstances:

- In the event of the successful bidder having been adjudged insolvent or going into liquidation or winding up their business or failing to observe any of the provisions of the contract or any of the terms and conditions governing the contract or failure to render the contracted services in time, HLL shall be at the liberty to terminate the contract forthwith without prejudice to any other right or remedies under the contract and to get the work done by other agencies at the risk and cost of the successful bidder and to claim from the successful bidder any resultant loss sustained or costs incurred.

- When the successful bidder is found to have made any false or fraudulent declaration or statement to get the contract or he is found to be indulging in unethical or unfair practices.
- When both parties mutually agree to terminate the contract.
- If the successful bidder transfers or assigns the contract or any part thereof to a third party, without the prior consent of HLL in writing.
- When there is a breach of contract

Part – IV

Scope of Work

Scope of Work for this RFP is defined below:

A. Cloud Infrastructure Design:

- The MSP shall design, deploy, install and configure the proposed infrastructure **(Annexure-1)** in the quoted Cloud Infrastructure for the smooth migration of SAP Applications of HLL from HLL Datacenter.

- MSP shall examine the application landscape that needs to be hosted on cloud infrastructure. This activity may enable the MSP to gauge the application workload requirements before provisioning the respective cloud infrastructure / services.

- MSP shall provide services from only one CSP during the entire tenure of the contract.

- However migration of SAP Applications is not under the scope of this RFP, MSP shall support the respective application teams for the deployment of HLL's SAP Applications on the cloud infrastructure.

- The MSP shall be responsible for provisioning of requisite network infrastructure and connectivity to ensure accessibility of the instances as per the defined SLA's.

- MSP shall set up and manage the entire cloud solution by provisioning and managing Cloud based resources. The Applications in the public domain like Employee Self Service (ESS) Portal shall be hosted in public subnet protected with Web Access Firewall (WAF).

- MSP shall provide a detailed solution document for setting up of the Cloud Environment and the same shall be approved by HLL before the deployment of services.

- MSP shall facilitate Security audit conducted by HLL based on HLL's audit policy. HLL reserves the right to get the cloud landscape audited by any third-party auditor, if deemed necessary.

- MSP shall enable the logs and monitoring as required to support for third party audits. The MSP needs to comply with the findings of the security audit in terms of the services provided under this RFP.

- The MSP shall carry out hardening of OS (Operating System), upgrade, patch and other configuration management activity on all OS and its related software etc., (which is provided under this RFP) as per the requirement of HLL's security audit observations during the Contract Period.

- The Cloud services shall be available on pay as per usage model. The billing shall be done monthly irrespective of Fixed, On- Demand or mixed model of the CSP.

- The MSP shall provide;

  i. Details of the monitoring & management tools and Helpdesk Solution.
  ii. Primary and secondary Contact details for support.
  iii. Escalation matrix to be adopted,
  iv. The detailed BOQ for Compute, Network, Storage, Security, Backup and all other components.
  v. High- and Low-Level Architectural Diagram of entire Setup
  vi. High- and Low-Level Network Diagram
  vii. Other required details.

- The MSP shall ensure that the proposed solution is as per the HLL requirement and satisfaction of the post migration & implementation of SAP Applications.

B. Infrastructure Analysis and Build

- MSP shall adequately size the necessary compute, storage and other cloud services required as listed in BOQ (**Annexure 1)** building the redundancy into the architecture and load balancing to meet the service levels.

- MSP shall advise on optimal operational practices, day-to-day & emergency procedures deploy & monitor underlying cloud services and performance reporting & metrics.

- MSP shall ensure the overall reliability and responsive operation of the underlying cloud services through both proactive planning and rapid situational response.
- The proposed cloud infrastructure/services provisioned by the MSP shall be scalable & flexible and HLL shall be able to add/reduce cloud infrastructure / services on demand basis
- MSP shall provide monitoring tools for measuring the service levels, application performance & utilization for instances, storage and network. The tool shall be capable of providing the exact utilization of instances and shall be able to generate per day, per month and per quarter utilization reports.
- MSP shall provide metering and billing to provide service assurance for maintenance & operations activities. The proposed Cloud infrastructure should have detailed user level or user group level auditing, monitoring, metering, accounting, quota and show-back information.
- MSP shall provide the Vulnerability Assessment (VA) report for instance in use in periodic basis.
- The CSP shall deploy instances on Server-Hardware having 1:2 Physical Core to vCPU ratio.
- The HANA DB shall be deployed in SAP HANA Certified instances as per sizing provided in BOQ (**Annexure 1)**.
- The instances shall be capable of running different operating systems (RHEL, Suse Linux, Windows etc.) with any of their versions.

C. Resource Management and Monitoring

- Based on the growth in the user load (peak and non-peak periods; year-on-year increase), the compute and storage as per the performance requirements of the solution shall be scaled up or scaled down.

- MSP shall carry out the scaling up / scaling down (beyond the auto-scaling limits or whenever the auto-scaling limits have to be changed) with prior approval from HLL.
- For every major change in cloud infrastructure, Change Management Procedure shall be followed with HLL's prior approval.
- MSP shall provide and implement tools and processes for monitoring the availability of assigned applications, responding to system outages with troubleshooting activities designed to identify and mitigate operational issues.
- MSP shall make provisions to monitor the network traffic in HLL's Cloud landscape and to analyze amount of data transferred (uploaded/ downloaded) via Internet traffic.
- MSP shall make provisions to monitor the uptime of all cloud resources and set threshold for alerts.MSP shall make provisions for setting alerts based on defined thresholds. There should be provision to configure different email addresses for sending alerts.
- MSP shall ensure that there should be historical data for a minimum of 12 months for resource utilization to resolve any billing/ audit disputes if any.
- MSP shall ensure that there are sufficient graphical reports of cloud resource utilization and available capacity.

D. Data Handling & Management

- HLL shall retain ownership of all data & application licenses hosted on CSP's infrastructure and shall be able to retrieve full copies of these at any time (without any charges).
- HLL retains ownership of all templates, clones, and scripts/applications created for HLL's applications. HLL retains the right to retrieve full copies of instances at any time (without any charges).
- HLL will own and deploy the licenses of all its SAP applications and HANA DB licenses for its SAP environment.

- The MSP shall provide and implement security mechanisms for handling data at rest and in transit. For this, MSP shall provide encryption mechanism.
- In the event of expiration / termination of the contract, MSP shall handover complete data in the desired format to HLL which can be easily accessible and readable without any additional cost. Data so received should be transportable to any other Public/Private cloud.

E. Administration, Configuration & Training

- The MSP shall facilitate Administration of users, identities, and authorizations, effectively managing the root account, as well as any Identity and Access Management (IAM) users, groups, and roles they associated with the user account.
- The MSP shall implement multi-factor authentication (MFA) for the root account, associated with it for cloud portal.
- Upon deployment of instances, the MSP must take full administrator access for the entire contract period (3 years) and is responsible for performing additional configuration, security hardening, vulnerability scanning, hardening, patch upgrades deployment etc. as and when required.
- MSP shall seek consent from HLL before doing any upgrade in OS/any services with detailed report of associated services / functionalities which may get impacted due to the upgrade.
- The MSP shall ensure Preparation and Updating of the new and existing Standard Operating Procedure (SOP) documents for Cloud based services.
- The MSP shall be setting up and configuring the instances as per configuration documents, guidelines, suggestions provided by HLL.
- The MSP shall provide training for HLL personnel on proposed cloud platform and Self-Service portal with respective certifications. The training shall be online or offline as per the requirements of HLL.HLL shall provide necessary arrangements for the offline training.

F. Security of Cloud Infrastructure

1 MSP shall ensure security of cloud services and infrastructure from any threats and vulnerabilities.

2 MSP shall address ongoing needs of security management including, but not limited to, monitoring of various devices / tools such as firewall, intrusion prevention/ detection, content filtering & blocking, virus protection, event logging & correlation and vulnerability protection through implementation of proper patches and rules.

3 MSP shall configure, monitor and regularly review the security services / configurations for the workloads deployed on Cloud.

4 MSP shall monitor the environment for unauthorized activity / access to the systems and conduct regular vulnerability scanning of the systems.

5 MSP shall provide security assessment report with respect to security configuration gaps and possible improvements to the security and compliance of cloud services on a quarterly basis.

6 MSP shall resolve any identified gaps / scope for improvement upon mutual consultation with HLL either as fixed or hence no longer a gap or acceptable risk and hence no further action required.

7 All the security management processes, tools and usage shall be well documented in security policy and the security best practices to be followed to maintain IT security.

G. Backup & Restoration

1 MSP shall configure, schedule, monitor and manage backups of all the data including but not limited to files, images and databases as per the policy finalized by HLL.

2 MSP shall restore the Application/Database from the backup whenever required.

Indicative Backup plan

Sl.No.	Backup Type	Backup Frequency	Retention
1	Incremental	Daily	7 Days
2	Full	Weekly	1 Month
3	Full	Monthly	3 Months
4	Transaction/ Archive logs	Every 1 Hour for Production instances, 3 Hours for other instances	2 Months

H MIS Reports

- MSP shall submit the reports on a regular basis in a mutually decided format.
- MSP shall prepare the formats for the MIS reports and send the same to HLL for approval soon after placing the Work Order.
- The following is only an indicative list of MIS reports that need to be submitted to HLL;

H.1 Weekly Reports

I. Summary of systems rebooted.

II. Summary of issues / complaints logged with the CSP.

III. Summary of changes undertaken for the cloud services including major changes like configuration changes, patch upgrades, etc. and minor changes like log truncation, volume expansion, user creation, user password reset, etc.

H.2 Monthly Reports

I. Component wise availability and Resource Utilization.

II. Consolidated SLA / Non- conformance report.

III. Summary of component wise uptime.

IV. Log of break-fix / preventive / scheduled maintenance undertaken.

V. All relevant reports required for calculation of SLAs.

VI. Any security incidents.

H.3 Quarterly Reports

I. Consolidated component-wise availability and resource utilization.

II. All relevant reports required for calculation of SLAs.

III The MIS reports shall be in-line with the SLAs and the same shall be scrutinized by HLL.

I. Disaster Recovery (DR) Solution

- MSP shall provide business continuity and disaster recovery services as per the service levels.
- The MSP shall configure the specified instances mentioned in the BOQ in Active-Active mode in DR Site (different physical location).
- The MSP shall configure the specified instances mentioned in the BOQ in Active-Passive mode in DR Site (different physical location). In case the primary environment goes down, the MSP shall scale up the specified DR instances for the services to be delivered without any change in performance with the required RPO and RTO as defined as follows;

Recovery Time Objective (RTO)	Measured during the regular planned or unplanned (outage) Change over from DC to DR or vice versa.	RTO <= 4 hours
Recovery Point Objective (RPO)	Measured during the regular planned or unplanned (outage) changeover from DC to DR or vice versa.	RPO <= 2 Minutes

- MSP shall configure, schedule, monitor and manage DR Drills as per the DR policy finalized by HLL.

J. Maintenance & Support of the Implemented Cloud Infrastructure

- The MSP shall be responsible for providing 24x7x365 days' support to the infrastructure from the date of issuance of operational acceptance by HLL, ensuring uptime and utilization of the cloud resources as per defined SLA.
- MSP shall deploy sufficient support persons suitably qualified and having experience in Coordinating & Managing Cloud Infrastructure during the entire duration of the contract in shifts to meet the defined SLA.
- MSP shall intimate HLL immediately about the surge in resource usage in case of DDoS or any other cyber-attacks.
- MSP shall develop reusable scripts to automate the process of infrastructure (like virtual machine, storage and network etc.) deployment and subsequent configuration for various use cases at no additional cost.
- The MSP must provide multiple support options catering to the varying levels of support requirements (e.g., support number, ticket) for HLL.
- The MSP shall develop appropriate policy, checklists etc. in line with ISO 27001 & ISO 20000 framework for failover and fallback to the appropriate DR site.

K. Indicative Service Levels

- CSP's **standard commercial** service levels (available on the public website) will be applicable for all the cloud services.
- The key service level objectives for managed services that relate to the cloud service and the related aspects of the interface between the HLL and the MSP are given as follows;

  I. The SLA parameters shall be monitored on a monthly basis as per the individual SLA parameter requirements. However, if the performance of the system/services is degraded significantly at any given point in time during the contract and if the immediate measures are not implemented and issues are not rectified to the complete satisfaction of Client, then the HLL will have the right to take appropriate disciplinary actions including termination of the contract.

II. The full set of service level reports should be available to HLL on a monthly basis or based on the project requirements.

III. In case these service levels cannot be achieved at service levels defined in the agreement, HLL shall invoke the performance related penalties. Payments to the MSP will be linked to the compliance with the SLA metrics laid down in the agreement.

IV. In case multiple SLA violations occur due to the same root cause or incident then the SLA that incurs the maximum penalty may be considered for penalty calculation rather than a sum of penalties for the applicable SLA violations.

V. Penalties shall not exceed 100% of the monthly bill. If the penalties exceed more than 50% of the total monthly bill, it will result in a material breach. In case of a material breach, the MSP will be given a cure period of one month to rectify the breach failing which a notice to terminate may be issued by the Client.

VI. Maximum cumulative penalty cannot exceed 10% of the work order value after which HLL may lead to the termination of the contract.

VII. Below severity definition provide indicative scenarios for defining incidents severity. However, User Department will define / change severity at the time of the incident or any time before the closure of the ticket based on the business and compliance impacts.

Severity Level	Description	Examples
Severity 1	**<u>Environment is down or major malfunction</u>** 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.	

L Exit Management

- CSP shall provide support to HLL for transferring data / applications at the time of exit management and as per the guidelines defined by MeitY in Cloud Services empanelment.
- CSP shall be responsible to keep the data on their cloud platform for minimum of 90 days in case of any dispute or account suspension. CSP has to provide the declaration on their letter head to confirm for the data to be saved on their cloud platform for 90 days.
- MSP shall assist HLL in migrating the data, network etc., and should ensure destruction of data, content and any other assets to the new environment or on alternate CSP's offerings and ensuring successful deployment and running of the solution on the new infrastructure by suitably retrieving all data, scripts, virtual machine images, and so forth to enable mirroring or copying to industry standard media.
- The ownership of the data generated upon usage of the system, at any point of time during the contract or expiry or termination of the contract, shall rest absolutely with HLL.
- Once the exit process is completed, remove the data, content and other assets from the cloud environment and destroy the VM, Content and data of HLL as per stipulations and shall ensure that the data cannot be forensically recovered

Sl. No	Service Level Objective	Definition	Target	Penalty
Availability				
1.	Availability of each cloud service (Applicable for all Cloud Services defined in the BOQ)	Availability means, the aggregate number of hours in a calendar month during which cloud service is actually available for use through command line interface, user/admin portal and APIs (which ever applicable) Uptime Calculation for the calendar month is as follows; {[(Uptime Hours in the calendar month + Scheduled Downtime in the calendar month) / Total No. of Hours in the calendar month] x100}	Availability for each of the cloud service >=99.9%	Penalty as indicated below (per occurrence): a) <99.9%to >=99.5%-10% of the total Monthly Payment. b) <99.5%to>=99 % -20% of the total Monthly Payment. c) <99% - 30% plus 10 % of the total Monthly Payment for each percentage drop below 99% In case the services is not available for a continuous period of 8 Business Hours on any day, penalty shall be 100% of the total Monthly Payment.
2.	Availability of the Cloud Management Portal of CSP	Availability means the aggregate number of hours in a calendar month during which cloud management portal of CSP is actually available for use	Availability >=99.9%	Penalty as indicated below (per occurrence): a) <99.9%to >=99.5%-10% of the total Monthly Payment.

		Uptime Calculation for the calendar month is as follows; {[(Uptime Hours in the calendar month + Scheduled Downtime in the calendar month) / Total No. of Hours in the calendar month] x100}		b) <99.5%to>=99 % -20% of the total Monthly Payment. c) <99% - 30% plus 10 % of the total monthly payment for each percentage drop below 99% In case the services is not available for a continuous period of 8 Business Hours on any day, penalty shall be 100% of the total Monthly Payment.
3	Provisioning of new Virtual Machine	Time to provision new Virtual Machine (up to 64 core) within 10 minutes (Measurement shall be done by analysing the log files)	Availability >= 95%	Penalty as indicated below (per occurrence): a) <95% to >= 90.00% - 5% of Monthly Payment of the Service. b) <90% - 10% plus 5 % of the monthly payment of the particular service for each percentage drop below 90%

4	Spinning up the Object Storage	Time to spin up Object Storage shall be within 15 minutes (Measurement shall be done by analysing the log files)	Availability >= 98%	Penalty as indicated below (per occurrence): a) <98% to >= 95.00% - 5% of Monthly Payment of the Service b) <95% to >= 90.0% - 10% of Monthly Payment of the Service c) <90% - 15% plus 5% of Monthly Payment of the Service for each percentage drop below 90%
5	Spinning up the Block Storage	Time to spin up to 100 GB Block Storage and attach it to the running VM within 15 minutes Measurement shall be done by analyzing the log files	Availability >=98%	Penalty as indicated below (per occurrence): a) <98% to >= 95.00% - 5% of Monthly Payment of the Service b) <95% to >= 90.0% - 10% of Monthly Payment of the Service d) <90% - 15% plus 5% of Monthly Payment of the Service for each percentage drop below 90%

Performance				
6.	Usage metric for all Cloud Services	The usage details for all the Cloud Service should be available within 15 mins of actual usage Measurement shall be done by analyzing the log files and Cloud Service reports.	Availability >=99%	Penalty as indicated below (per occurrence): a) <99% to >= 95.00% - 1% of the total Monthly Payment b) <95% to >= 90.0% - 2% of the total Monthly Payment. c) <90% - 3% plus 1% of the total Monthly Payment for each percentage drop below 90%
7.	Usage cost for all Cloud Service	The cost details associated with the actual usage of all the Cloud Service should be available within 24Hrs of actual usage Measurement shall be done by analyzing the log files and Cloud Service reports and Invoices	Not more than 24 Hrs. of lag between availability of cost details and actual usage. Availability >=99%	Penalty as indicated below (per occurrence): a) <99% to >= 95.00% - 1% of the total Monthly Payment. b) <95% to >= 90.0% - 2% of the total Monthly Payment. c) <90% - 3% plus 1% of the total Monthly Payment for each percentage drop below 90%

Security				
8	Percentage of timely vulnerability reports	Percentage of timely vulnerability reports shared by CSP/MSP with HLL within 5 working days of vulnerability identification. Measurement period is calendar month.	Percentage of timely vulnerability reports within 5 working days of vulnerability identification >= 99.95%	Penalty as indicated below (per occurrence): a) <99.95% to >= 99.00% - 10% of the total Monthly Payment. b) <99.00% - 20% plus 5% of the total Monthly Payment for each percentage drop below 99 %
9	Percentage of timely vulnerability corrections	Percentage of timely vulnerability corrections performed by CSP/MSP. High Severity – Perform vulnerability correction within 30 days of vulnerability identification. Medium Severity – Perform vulnerability correction within 60 days of vulnerability identification. Low Severity – Perform vulnerability correction within 90 days of vulnerability identification. Measurement period is calendar month.	Maintain 99.95% service level	Penalty as indicated below (per occurrence): a) <99.95% to >= 99.00% - 10% of the Monthly Payment. b) <99.00% -20% plus 10 % of total Monthly Payment for each percentage drop below 99%
10	Security breach including Data	Any incident wherein system including all cloud based services and components are compromised or any case wherein data	No breach	For each breach/data theft, penalty will be levied as per following criteria.

	Theft/Loss/Corruption	theft occurs (includes incidents pertaining to CSPs only)		Penalty of Rs 10 Lakh 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, HLL reserves the right to terminate the contract.
11	Security Incident (Malware Attack/ Denial of Service Attack/ Data Theft/ Loss of data/ Intrusion or Defacement) Applicable on the CSP's underlying infrastructure	Security incidents could consist of any of the following: Malware Attack: This shall include Malicious code infection of any of the resources, including physical and virtual infrastructure and applications. Denial of Service Attack: This shall include nonavailability of any of the Cloud Service due to attacks that consume related resources. CSP shall be responsible for monitoring, detecting and resolving all Denial of Service (DoS) attacks. Intrusion: Successful unauthorized access to system, resulting in loss of confidentiality/ Integrity/availability of data. CSP shall be responsible for monitoring, detecting and resolving all	Any Denial of service attack shall not lead to complete Service nonavailability. Zero Malware attack / Denial of Service attack / Intrusion /Data Theft	For each occurrence of any of the attacks (Malware attack / Denial of Service attack / Intrusion / Data Theft), 10% of the total Monthly Payment.

		security related intrusions on the network using an Intrusion Prevention device		
Support Channels - Incident and Helpdesk				
12 .	Response Time under Basic Support (As defined under cloud service bouquet)	Average Time taken to acknowledge and respond is within 15 Minutes, 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% - 5% plus 1 % of the total Monthly Payment for each percentage drop below 95%
13	Time to Resolve - Severity 1	Time taken to resolve the reported ticket / incident from the time of logging.	For Severity 1, 99% of the incidents should be resolved within 30 minutes of problem reporting	• < 99% &>= 97% (5% of the Monthly Payment) • < 97% &>= 95% (10% of the monthly Payment). • < 95% (15% plus 1% of the Monthly payment for each percentage drop below 95%)
14	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	a) < 95% &>= 90% (2% of the Monthly Payment) b) < 90% &>= 85% (4% of the Monthly Payment) c) < 85% (6% plus 1% of the Monthly payment for each percentage drop below 85%)

Audit & Monitoring				
15.	Patch Application	Patch Application and updates to underlying infrastructure and cloud service Measurement shall be done by analyzing security audit reports	95% within 8 Hrs. of the notification	Penalty as indicated below (per occurrence): a) <95% to >= 90.00% - 5% of Monthly Payment of the Project b) <90% to >= 85.0% - 10% of Monthly Payment of the Project c) <85% to >= 80.0% - 15% of Monthly Payment of the Project d) <80% - 20% of the Monthly Payment of that Project
16	Alerts & Notification	Alerts and Notifications for usage based threshold Measurement shall be done by analyzing the log files	99% within 10 mins of crossing the Threshold	Penalty as indicated below (per occurrence): a) <99% to >= 95.00% - 0.25% of Monthly Payment of the Project b) <95% to >= 90.0% - 0.5% of Monthly Payment of the Project c) <90% to >= 85.0% - 0.75% of Monthly Payment of the Project d) <85% - 1% of the Monthly Payment of that Project

17	Non-closure of Audit observations	No observation to be repeated in the next audit	All audit observations to be closed within defined timelines	Penalty for percentage of audit observations repeated in the next audit a) > 0 % &<= 10% - 5% of the total Monthly Payment b) > 10 % &<= 20% - 10% of the total Monthly Payment. c) > 20 % &<= 30% - 20% of the total Monthly Payment. d) >30% - 30% plus 5% of the total Monthly Payment for each increase in percentage from 30 %.

Part – V

Forms & Annexures

Annexure-1

Bill of Quantity (BOQ)

Name of Bidder :-

Sl No	Item Description	Qty	Unit	CSP Public Listed Price Per Unit To be entered by the Bidder in Rs.	Qty (In Hours)	CSP Service Name To be entered by the Bidder	CSP Website Link To be entered by the Bidder	Total Contract Duration (In Months)	Total CSP Public Listed price (monthly in INR)
		A		B	C			D	E = A*B*C*D
1	**Compute Services**								
1.1	Intel Latest Processor Based Virtual machine (Enterprise Grade Linux for SAP Applications - RHEL/Suse included) **CSP Service Specifications:** Linux VM 16 vCPU 64GB RAM 100GB SSD	6	Per hour		730			36	
1.2	Intel Latest Processor Based Virtual machine (Enterprise Grade Linux for SAP Applications- RHEL/Suse included) CSP Service Specifications: Linux VM 4 vCPU 16GB RAM 100GB SSD	21	Per hour		120			36	

1.3	Intel Processor Based Virtual machine (Enterprise Grade Linux for SAP Applications- RHEL/Suse included) CSP Service Specifications: Linux VM 2 vCPU 8GB RAM 650GB SSD	4	Per hour		730			36	
1.4	Intel Processor Based Virtual machine (Enterprise Grade Linux for SAP Applications - RHEL/Suse included) **CSP Service Specifications:** Linux VM 128 vCPU 1TB RAM 100GB SSD	3	Per hour		730			36	
1.5	Intel Processor Based Virtual machine (Enterprise Grade Linux for SAP Applications- RHEL/Suse included) **CSP Service Specifications:** Linux VM 128 vCPU 2TB RAM 100GB SSD	1	Per hour		730			36	
1.6	Intel Processor Based Virtual machine (Enterprise Grade Linux for SAP Applications- RHEL/Suse included) **CSP Service Specifications:** Linux VM 64 vCPU 384GB RAM 100GB SSD	2	Per hour		730			36	
1.7	Intel Processor Based Virtual machine (Enterprise Grade Linux for SAP Applications- RHEL/Suse included) CSP Service Specifications: Linux VM 32 vCPU 384GB RAM 100GB SSD	2	Per hour		120			36	
1.8	Intel Processor Based Linux virtual machine (Enterprise grade Linux with Enterprise support included for the OS) License included **CSP Service Specifications:** Linux VM 64 vCPU 512GB RAM 100GB SSD	2	Per hour		120			36	

1.9	Intel Processor Based Linux virtual machine (Enterprise grade Linux with Enterprise support included for the OS) License included**CSP Service Specifications:** Linux VM 48 vCPU 1TB RAM 100GB SSD	1	Per hour		120			36	
1.10	Intel Processor Based Linux virtual machine (Enterprise grade Linux with Enterprise support included for the OS) License included **CSP Service Specifications:** Linux VM 8 vCPU 32GB RAM, 100 GB SSD	13	Per hour		120			36	
2	**Storage**								
2.1	Permanent non-ephemeral Block storage (Solid State Drive designed to offer minimum 7500 IOPS and 1000 MB/s of throughput per volume) **CSP Service Specifications:500 GB per VM. (20 VMs)**	10	Per TB per month		730			36	
2.2	Permanent non-ephemeral Block storage (Solid State Drive designed to offer minimum 7500 IOPS and 1000 MB/s of throughput per volume) **CSP Service Specifications:300 GB per VM. (10 VMs)**	3	Per TB per month		730			36	
2.3	Permanent non-ephemeral Block storage (Solid State Drive designed to offer minimum 7500 IOPS and 1000 MB/s of throughput per volume) **CSP Service Specifications:200 GB per VM. (10 VMs)**	2	Per TB per month		730			36	
2.4	Shared File Storage (NFS) for Linux with Redundancy in same site with three redundant copies over SSD. **CSP Service Specifications:** 5TB of Shared File Storage (NFS)	5	Per TB per month		730			36	

2.5	Object Storage with Redundancy across zones/sites with storage durability of 99.999999999% **CSP Service Specifications:** 5TB of Object Storage in redundancy across 3 different physical locations	5	Per TB per month		730			36	
2.6	SSD Snapshot in Zone/Multi-Site redundant storage CSP Service Specifications: 500 GB Per VM Snapshot (20 VMs) 10% data changed every month	1	Per TB per month		730			36	
2.7	Archival Storage with redundancy across zones/sites with storage durability of 99.999999999% able to restore file within 5 - 12 hours **CSP Service Specifications:** 10TB of Archival Storage in redundancy across 3 different physical locations	10	Per TB per month		730			36	
2.8	Permanent non-ephemeral Block storage (Solid State Drive designed to offer minimum 3000 IOPS and 125 MB/s of throughput per volume) **CSP Service Specifications:500 GB per VM. (20 VMs)**	10	Per TB per month		40			36	
3	**Network**								
3.1	Load Balancers having 2 rules evaluating for every request with data being processed up to 1TB/month and 1/MN request/month **CSP Service Specifications:** 2 Load balancer unit for Layer 7 load balancing	2	Load Balancer / month		730			36	
3.2	Gateway can connect to multiple attachment types such as Virtual Private Clouds, Direct Connect and VPNs **CSP Service Specifications:** 10 attachments and 2TB data processed per gateway	10	Attachm ents		730			36	

3.3	Data Transfer Egress from Compute & database directly to internet **CSP Service Specifications**: 1TB DTO out per month from provision compute capacity.	1	Per TB per month		730			36	
3.4	Data Transfer between the sites for the replication **CSP Service Specifications**: 1TB DTO out per month from provision compute capacity.	3	Per TB per month		730			36	
3.5	Managed Network out gateway for secure internet access **CSP Service Specifications:** 2 count of Managed NAT service with capacity of 100 GB data per month	2	Gateway /month		730			36	
4	**Security Services**								
4.1	Basic Firewall with Access Control (IP-PORT Based) **CSP Service Specifications:** Setting up inbound and outbound rule based on ip address and port basic. With 250GB Data Processed in a month	2	Per Subnet /Per Month		730			36	
4.2	Cloud native service to monitor and records account activity across infrastructure	1	Per month		730			36	
4.3	Cloud security posture management service to perform security best practice, aggregates alerts, and enables automated remediation.	1	Per month		730			36	
4.4	Managed Threat Detection Service that uses intelligence, machine learning and advanced features to continuously monitors for malicious activity and unauthorized behaviour to monitor the cloud resources	1	Per month		730			36	

4.5	Cloud native security vulnerability assessment service	1	Per month /Per Instances		20			36	
4.6	FIPS 140-level 3 cloud managed self-serve provisioning HSM unit. Proposed HSM should be a managed service of same cloud service provider for ease of integrations, manageability, and deeper integration with rest of the services. Should be able to provide availability of HSM within 1 hour, in case of any failure of HSM unit.	1	No of HSM device unit per month		730			36	
4.7	WAF Firewall CSP Service Specifications: 10 WAF with 10 rules each having 100MN hits per month	10	Monthly		730			36	
4.8	Should provide DDoS protection for managed services endpoints. Can be used with CDN and provide comprehensive protection against all known infrastructure (Layer 3 and 4) attacks. Should provide always-on detection and automatic inline mitigations, minimize application downtime and latency.**CSP Service Specifications:** Per resource Per Month for 300 resources (300 Public Ip address)	1	Monthly		730			36	
4.9	VPN Connectivity (Provisioned for two different ISP's - Active-Active configuration) as Site-to-Site VPN (available as a managed service from CSP) with upto 1.25 Gbps bandwidth per VPN tunnel **CSP Service Specifications:** VPN connection with throughput of 1.25 Gbps	10	No of unit Per Month		730			36	

4.10	Client VPN Services (IPSEC VPN Tunnel for Remote/Roaming Users)	300	No of unit Per Month		200			36	
P	Total List Price (Sum of Column **E**) in Rs.								
Q	Discount offered by Bidder on CSP Public listed Price in Percentage (% of **P**)								
R	Discount offered by Bidder on CSP Public listed Price in Rs								
S	Total Quoted Price (**P - R**)								
T	Cost for Managed Services in Percentage (% of **S**)								
U	Cost for Managed Services in Rs								
V	One Time implementation Charges if any in Rs								
W	Net Price (**S + U + V**)								

Annexure-2

NON-DISCLOSURE AGREEMENT

M/s HLL Lifecare Limited, (CIN ……………) Poojappura P O, Thiruvananthapuram-695012, (hereinafter called M/s HLL) has entered into a contract with M/s(Company Name), with its registered office at (Office address), (hereinafter called M/s (Company Name in Short) for the "Installation, Configuration and Maintenance of Cloud Based Infrastructure for hosting the SAP Applications of HLL " in HLL, by placing Purchase Order (PO) (PO number) dt.(PO date) for an amount of RS.(PO Amount) on M/s(Company Name). As per confidentiality Clause (Clause no) of the PO, a Non-disclosure agreement has to be signed between M/s (Company Name) and M/s HLL for complying the same without any level of dilution.

This Non-Disclosure Agreement, dated as of (Agreement date) is made and signed between M/s HLL and M/s (Company Name) in connection with the Installation, Configuration and Maintenance of Cloud Based Infrastructure for hosting the SAP Applications of HLL. M/s (Company Name) means any person employed by M/s(Company Name) either directly or through their sub-contractors or provisional employees or trainees working for the Installation, Configuration and Maintenance of Cloud Based Infrastructure for hosting the SAP Applications of HLL and M/s HLL means any person of HLL employed either directly or through their sub-contractors or provisional employees working for HLL. In this Agreement, unless the context otherwise requires. M/s HLL and M/s (Company Name) shall hereinafter be jointly referred to as the "Parties" and individually as the "Party"- The Party hereinafter disclosing information shall be referred to as the "Disclosing Party" and the Party hereinafter receiving information shall be referred to as the "Recipient" or "Receiving Party".

The Non-disclosure agreement covers the following;

a) Information relating to the Installation, Configuration and Maintenance of Cloud Based Infrastructure for hosting the SAP Applications of HLLat M/s HLL shall not be disclosed by M/s (Company Name) to any agency or any other persons not officially concerned with such process. The undue use by M/s(Company Name) of confidential information related to the process may be treated as breach of confidentiality and dealt with accordingly. Except with the prior written consent of M/s HLL, M/s (Company Name) shall not at any time communicate either in hard copy form or electronic means or in any other mode to any other organization, person or entity any confidential information acquired in the course of the contract.

b) Neither Party will disclose to any third party without the prior written permission consent of the other party any confidential information which is received from the other party for the purpose of providing or receiving services.

c) Each party will take measures to protect the confidential information of the other party that, in the aggregate are no less protective than those measures it uses to protect the confidentiality of its own comparable confidential information, and in any event, not less than a reasonable degree of protection. Both parties agree that any confidential information received from other party shall only be used for the purpose of providing or receiving services under the above referenced contract for Installation, Configuration and Maintenance of Cloud Based Infrastructure for hosting the SAP Applications of HLL.

In this agreement "Confidential Information" shall mean any information relating to the Disclosing Party's business, commercial information or any information of a technical nature comprising inter alia products, processes, methodologies, frameworks, models, ideas, interpretations, Legal, technical and other documents, manuals, tariffs, standards, software, discs, reports, research, working notes, papers, data or information in wired or wireless mode, drawings, layout , data and techniques used by/owned by "HLL Lifecare Limited" in connection with Installation, Configuration and Maintenance of Cloud Based Infrastructure for hosting the SAP Applications of HLL in whatever form, provided all oral disclosure of confidential information is submitted by the Disclosing Party in writing to the Recipient within 30 (thirty) days, indicating compliance to the terms of this agreement.

In due consideration of the above, HLL Lifecare Limited granting M/s (Company Name) access to the Confidential Information and vice-versa, the Parties undertake that:

1. Subject to Clause 8 below, the Recipient will keep the Confidential Information strictly confidential and will not disclose it to any third party without the Disclosing Party's prior written consent, at any point of time.

2. Confidential Information will be disclosed only to those personnel and permitted assigns of the Recipient who need access to the Confidential Information for the proper performance of their duties in relation to the project and only to the extent necessary for the purpose of with Installation, Configuration and Maintenance of Cloud Based Infrastructure for hosting the SAP Applications of HLL. The Recipient, will solemnly take required steps appropriately in all means to ensure that all personnel to whom access to the Information is given are aware of its confidentiality and that they are bound by restrictions at least as onerous as those placed on the Parties by the terms of this agreement.

3. The Parties acknowledge that some or all of the Information is or may be price sensitive information and that the use of such information may be regulated or prohibited by applicable legislations and the Recipient undertakes not to use any such Information for any unlawful purpose. On acquiring any Confidential Information, the Recipient shall comply with all applicable laws in India in relation to insider trading and otherwise the acquisition of securities.

4. The Recipient agree to indemnify and hold harmless the Disclosing Party, its partners and staff and any of the Disclosing Party's clients to whom the Information relates against all loss, damage and expense (including legal expenses relating to any actions, proceedings and claims brought or threatened) of whatsoever nature and howsoever arising out of any breach by the Recipient of the confidentiality obligations under this Agreement.

5. Confidential Information disclosed to the Recipient will be used solely for the purpose of Installation, Configuration and Maintenance of Cloud Based Infrastructure for hosting the SAP Applications of HLL.

6. The Recipient shall establish and maintain all reasonable security measures to provide for the safe custody of the Information in whatever form it may be and to prevent unauthorized access to it.

7. This Agreement shall remain in effect for 10 years from the Effective Date of this Agreement ("Term"). On completion of with Installation, Configuration and Maintenance of Cloud Based Infrastructure for hosting the SAP Applications of HLL, the Recipient shall return all the Confidential Information disclosed to the Recipient and any copies thereof in whatever form it may be including soft copies, electronic forms to the Discloser.

8. The obligations contained above shall not apply to any Information which
   a. is or subsequently comes into the public domain otherwise than through a breach of this agreement;
   b. is already rightfully in the Recipient's possession;
   c. is obtained by the Recipient from a third party without any restriction on disclosure;
   d. The Recipient required to disclose by law or professional or regulatory obligation with the Disclosing Party's prior written consent.

9. Each party shall be responsible for any breach of this Agreement by any of their respective Representatives. If the Recipient becomes aware of any breach of confidence or threatened breach of confidence by any of the Recipient's direct employees or provisional employees including trainees or agents or sub-contractors, the Recipient will promptly notify the Disclosing Party of the same and give the Disclosing Party all reasonable assistance in connection with any proceedings which the Disclosing Party may institute against such persons. In case of breach of confidence, the damages will be assessed by the discloser and compensation claimed from the recipient as per the suitable laws as applicable in India including Indian Penal Code, Information Technology Act 2000, Intellectual Property law, Indian Contract Act, company laws and the jurisdiction for all such proceedings will be at the courts at Thiruvananthapuram.

10. The Recipient shall comply with the obligations set out herein throughout the tenure of contract and thereafter.

11. The Recipient acknowledges that the Disclosing Party shall retain the copyright and intellectual property rights in the Confidential Information and that the Receiving

Party shall not copy, adapt, transmit through wired media or wireless media, modify or amend full or any part of the Confidential Information or otherwise deal with any part of the Confidential Information except with the prior express written consent of Disclosing Party during period of the above contract.

12. This Agreement shall be fully governed by and construed in accordance with the relevant laws of India.

13. Notices: Any notice, claim or demand in connection with this agreement shall be given in writing to the relevant party at the address set out herein and sent by letter/fax shall be deemed received when properly sent, any notice sent by hand shall be deemed received when actually delivered and any notice sent by post shall be deemed received 72 hours after posting. A copy of all notices/replies sent between M/s HLL and M/s (Company Name) shall be emailed to (Company mail id) &udaya@lifecarehll.com respectively.

For M/s HLL Lifecare Limited	For M/s (Company Name)
AVP (IT)	Business Head
Witness: 1	Witness: 1
Witness: 2	Witness: 2

Annexure-3

FORMAT OF PERFORMANCE BANK GUARANTEE

To

HLL Lifecare LTD
HLL Bhavan
Mahilamandiram Road, Poojappura PO
Thiruvananthapuram, Kerala -695012.

WHEREAS …………………… (Name & Address of Contractor) (Hereinafter called "**the Contractor**") has undertaken, in pursuance of Contract……………………………… No.……………………Dated: ………………………… to execute ………………………… (Name of Contract and brief description of works) (Hereinafter called "**the Contract**").

AND WHEREAS it has been stipulated by **HLL Lifecare LTD** (The Purchaser – hereinafter called "**HLL**") in the said contract that the Contractor shall furnish HLL with a Bank Guarantee for the sum specified therein as security for compliance with the Contractor’s obligations in accordance with the Contract.

AND WHEREAS we have agreed to give the Contractor such a Bank Guarantee.
NOW THEREFORE we …………….. (Name of the Bank) having its Head Office at ……………………… (Address of Head Office) and acting through its branch office at …………………… (Address of the executing branch) (Hereinafter called "the Bank") hereby affirm that we are the Guarantor and responsible to **HLL**, on behalf of the Contractor up to a total of ………………………… (amount of Guarantee) …………………………in words).

NOW THEREFORE................................ (Name of the Bank) having its Head Office at......................... (Address of Head Office) and acting through its branch office at...................... (Address of the executing branch) (Hereinafter called "the Bank") hereby affirm that we are the Guarantor and responsible to **HLL**, on behalf of the Contractor up to a total of... (amount of Guarantee) in words).

We, the bank, hereby irrevocably undertake to pay you any amount not exceeding in total the Guarantee Amount upon receipt by us of your demand in writing accompanied by the following documents:

1. Your signed statement certifying that the Contractor is in breach of his obligation(s) under the Contract and the respect in which the Contractor is in breach.
2. Your signed statement certifying that the Contractor has been given a prior written notice by email from you to make good the aforesaid breach and that the Contractor still failed to fulfil the Contract within 30 days of such notice. A copy of such notice given by email to the Contractor shall be attached to the demand for payment.

Any demand for payment should contain your authorized signatures which must be authorized by your bankers or by a notary public.

We, the Bank, further agree that no change or addition to or other modification of the terms of the Contract or of the Works to be performed there under or of any of the Contract documents which may be made between **HLL** and the Contractor shall in any way release us from any liability under this guarantee, and we hereby waive notice of any such change, addition or modification. We, the Bank, further agree that any change in the constitution of the said contractor or the said bank shall not discharge our liability hereunder.

Notwithstanding anything contained herein:

1. Our liability under this Bank Guarantee shall not exceed.............................. (.......................... only).
2. This Bank Guarantee shall be valid up to (date) and
3. We are liable to pay the guaranteed amount or any part thereof under this bank guarantee only and only if **HLL** serve upon us a written claim or demand on or before ....(validity date) .

Any demand for payment under this guarantee must be received by us at this office during working hours on or before the validity date. Should we receive no claim from you by the validity date, our liability to you will cease and the guarantee will definitely become null and void whether returned to us or not.

Yours truly,
Signature and seal of the guarantor: ....

Name of Bank:..

Address: ....
Date:.......................................

[1] An amount shall be inserted by the Guarantor, representing the percentage of the Contract Price specified in the Contract and denominated in respective Indian Rupees.

Form A1

FORM A1:- Pre-qualification criteria compliance checklist

Eligibility Criteria of the MSP			
Sl. No	**Criteria**	**Docs Requested**	**Compliance Yes/No**
1	The bidder shall be a Indian Company/Firm in continuous business of the Hosting & Maintenance of Cloud infrastructure for the last Five (5)Years and registered under either ; • The Indian Companies Act, 2013 OR • A partnership firm registered under the Limited Liability Partnerships (LLP) Act, 2008 OR • A partnership firm registered under the Indian Partnership Act, 1932.	Copy of valid Certificate of Incorporation or Certified copy of valid Partnership Deed.	
2	The bidder should have all the following Experience in India during the last Five (5) Years prior to the Bid Submission Date; • Minimum **Five** (5) successful implementation of Cloud Environment. • Minimum **One** (1) successful implementation of Cloud Environment with order value greater than Rs. 50 Lakh **or** Minimum	Documentary evidences like Work Orders, Installation Certificates, and Client Certificate etc. for the same should be attached along with the bid.	

	Two (2) successful implementations of Cloud Environment with order value greater than Rs. 25 Lakh. - Minimum **Two** (2) Nos. of successful implementations of Cloud Environment in PSU/Central Govt/State Govt. - Minimum **One** (1) No. successful implementation of Cloud Environment for SAP Applications (ECC/S4HANA)		
3	The Bidder should have minimum average annual turnover of Rs. 50 Crores from IT Services during the last three Financial Years. i.e. (2019-20, 2020-21 and 2021-22).	Audited Balance Sheets and Profit & Loss account for the last three financial years and certificate from the statutory auditor shall be submitted. If the turnover is from fields other than IT services, then certificate from statutory auditor to be submitted for turnover from IT services separately (Supported with Form A6 certified by statutory auditor).	
4	The bidder should not have been blacklisted in past three years by any state/central Government Organizations / Firms / Institutions	Self-certificate stating that the bidder has not been blacklisted by any institution of the Central/ State Government	

5	The bidder should be regular tax payer under the Income Tax Act.	Details of PAN, GST etc.	
6	The bidder should have at least 10 Nos. of Professionals with certifications of the proposed Cloud Service Provider.	Details of such 10 Nos. of professionals shall be attached along with the bid	
7	The bidder should have certified for ISO 9001, ISO 20000 and ISO 27001.	Documentary evidences for the same should be attached along with the bid	
8	The bidder should be an authorized partner of the proposed Cloud Service Provider.	Authorization letter from the quoted CSP shall be submitted along with the bid.	
Eligibility Criteria of the CSP			
Sl. No	**Criteria**	**Docs Requested**	**Compliance Yes/No**
1	Proposed CSP should be an Indian Company registered under the Indian Companies Act, 2013.	Copy of valid Certificate of Incorporation	
2	Proposed CSP and offered facilities for DC&DR should have been ; • Empaneled by Ministry of Electronics and Information Technology (MeitY) for the last 3 years. And • STQC audited as per MeitY empanelment process as on the last date of submission of the bid.	Self-certified copy of MeitY, Government of India empanelment as CSP.	
3	Proposed CSP should have accreditations relevant to security, availability, confidentiality, processing integrity, and privacy Trust Services principles SOC 1, SOC 2 and SOC 3	Self-declaration from the Authorized signatory of the CSP on their letterhead.	

4	CSP must not have been blacklisted by a Central & State Government Institution/PSUs in India.	Self-declaration from the Authorized signatory of the CSP on their letterhead.	
5	Proposed CSP shall have an average turnover from cloud services in India of Rs. 2000 Crore in the last three (3) financial years i.e. (2019-20, 2020-21 and 2021-22).	Audited Balance Sheets and Profit & Loss account for the last three financial years and certificate from the statutory auditor shall be submitted. If the turnover is from fields other than IT services, then certificate from statutory auditor to be submitted for turnover from IT services separately (Supported with Form A6 certified by statutory auditor).	
6	Proposed CSP should be certified for ISO 27001, ISO 27017 and ISO 27018, ISO 22301, 27701:2019	Copy of Valid Certificates	
7	Proposed Cloud Solution to be deployed across different physical locations, with active-active configuration to ensure fault tolerance with high availability between two physical sites.	Self-certificate from the Authorized signatory of the CSP on their letterhead.	
8	CSP should have minimum 3 Nos. of MeitY empaneled and STQC audited data centers in physically different locations in India.	Self-certificate from the authorized signatory of the CSP on their letterhead confirming that they have 3 data centers in India. The same should be confirmed from the MeitY website as well.	
9	CSP should be in continuous business of the Hosting and Maintenance of Cloud infrastructure in India for more than **Five (5)** years prior to the bid opening.	Self-Certificate from the Authorized signatory of the CSP on their letterhead.	

10	CSP should have SAP-certified instances for running SAP HANA DB. Information about the instance types that are certified and supported for SAP should be available in public domain reference link	Self-Declaration from the Authorized signatory of the CSP on their letterhead.& Public Referenceable link	
11	CSP should offer multiple pricing models such as Pay-As-You-Go, Reserved and other such models for helping optimization of cost.	Self-certified letter from CSP on their letterhead.	
12	CSP should have published on its public facing website about cloud services' rates for India, Service Level Agreements (SLAs), dashboard live-status of cloud services' health across global datacenter and outage details (if any) with RCA	Self-certified letter from CSP on their letterhead.	

Form A2

FORM A2: Details of the Bidder (on Letterhead)

Sl No.	Particulars	Details	
1	Name of the Bidder		
2	Address of the Registered office		
3	Date of registration as Company/Firm		
4	Key Management Personnel		
5	Project Manager for HLL Project		
6	Contact Person for Bid related intimation Name : Designation : Email : Mobile No:		
7	Turnover from IT services for last three financial years (Supported with Audited Balance Sheet and Profit & Loss Account or Annual Report for the last three financial years)	2019-20	
		2020-21	
		2021-22	
8	PAN (Copy to be attached and specify page No)		
9	GSTIN (Copy of to be attached and specify page No)		
10	CSP Partner /contract certificate (Attach documentary proof in support and specify page No)		
11	ISO 9001, 20000 &27001 Certification (Attach documentary proof in support and specify page No)		

We hereby declare that all the information and statements made in this proposal are true and accept that any misrepresentation contained in it may lead to our disqualification.

Date:	Authorized Representative Signature:
Place:	Name:
Designation:	
Company Name:	
Seal of Company	

FORM A3: Financial Capability Report

Sl. No.	Financial Year	Annual Revenue / Turnover from IT services	Net worth as at the end of the financial year
1	2019-20		
2	2020-21		
3	2021-22		

*Attach separate work sheet if required.

Date:	Authorized Representative Signature:
Place:	Name:
Designation:	
Company Name:	
Seal of Company	

FORM A4: Letter of Confirmation / Declaration

LETTER OF CONFIRMATION / DECLARATION

To,
The Associate Vice President (IT)
Corporate and Registered Office
HLL Lifecare Limited
Poojappura P.O., Kerala, India - 695012

RFP Ref. No.:-

Dear Sir/Madam,

We confirm that we will abide by the conditions mentioned in the Tender Document (RFP and annexure) in full and without any deviation.

We shall observe confidentiality of all the information passed on to us in course of the any Review /Audit process and shall not use the information for any other purpose than the current tender.

We confirm that we have not been black listed/banned in last three years, from the date of floating of the RFP or at the time of submission of Tender, by any State/Central Government organizations /Firms / Institutions/ Central PSU / PSE.

Date:	Authorized Representative Signature:
Place:	Name:
Designation:	
Company Name:	
Seal of Company	

Form A5

FORM A5: Compliance Checklist

We, M/s ………………………………………………hereby solemnly confirm and declare that we have gone through the entire tender document / instructions, Scope of Work, Project Schedule, Prequalification criteria, General terms and conditions and all other documents attached to the RFP ……………………………………of M/s HLL Lifecare Ltd, in detail and full. Entire specifications, Scope of Work, Prequalification criteria, Technical Evaluation Criteria, Project Schedule, instructions, terms and conditions are noted and understood and get clarified with M/s HLL Lifecare Ltd. and submitting the offer herewith.

We hereby confirm.

Sl No	DESCRIPTION	COMPLIANCE		Page No in the Offer
		Yes	No	
1	It is confirmed that scope of works in detail as per Part -IV of this document is noted and accepted.			
2	It is confirmed that Project Plan and Technical Compliance Statement as per the bid are noted and accepted.			
3	It is confirmed that the Qualification criteria for bidders as per Part –III clause 3.1 & 3.2 of this document is noted and submitted filled and duly signed along with the offer.			
4	It is confirmed that the Forms A1 to A3 of this document required as per the qualification criteria and copy of documentary proofs in this regard submitted (filled and duly signed) along with the offer.			
5	Letter of confirmation/ declaration as per Form A4 of this document submitted as required.			
6	CSP Partner certification documentary proof submitted.			
7	Valid ISO 9001, ISO 20000 and ISO 27001 certification, as on releasing date of RFP.			
8	Project Manager CV and experience details submitted as required.			
9	Documentary proof of list of 10 professionals on roll with certifications in the proposed CSP to be deputed exclusively for HLL project along with their qualification and experience.			

10	Bid evaluation criteria as per Part –III clause 12.5 of this document and terms of payment as per part III Clause-22 of this document is noted and accepted.			
11	It is confirmed that the EMD, instructions and general terms & conditions as per Part-II & Part –III of this document are read and understood.			
12	Self-attested copy of PAN card under Income Tax Act submitted.			
13	Self-attested copy of GST registration number and details submitted.			
14	NEFT mandate form and cancelled cheque as per Form A7 of this document.			
15	VALID copy of MSME/NSIC Registration Certificate along with the list of items / services for which they are registered, as issued by NSIC for EMD exception, if applicable.			
16	Start-up Registration certificate as defined under notification of DIPP GSR 501(E) dated 23 May 2017 for availing the specified relaxations if applicable.			
17	It is confirmed that Original tender document read and understood completely and submitted a copy duly signed and sealed on all pages.			
18	EMD payment details as per Part-III Clause 20 submitted along with the technical bid document as required in the tender.			
19	Copy of un-priced bid format as per Form-A10 (price bid WITHOUT prices/numerals) submitted.			

We, M/s ……………………………………………..solemnly reconfirm and declare that the above checklist points elicited are fully known to us and we hereby confirm its compliances in full for the entire project period including its guarantee period. It is also confirms that we will consider and implement the detailed specification in the RFP and points in this check list are considered as reaffirmation of those points in concise form. I the undersigned hereby truly confirm that I am authorized to sign on this document as per articles of association of M/s …………………………. where I am employed as per the details given along with my signature below.

Date:	Authorized Representative Signature:
Place:	Name:
Designation:	
Company Name:	
Seal of Company	

FORM A6: Technical Compliance Statement

Sl. No.	Minimum Requirement	Compliance Yes/ No	Service Names and URL of the services for description
1.	**Virtual Machine or Compute**		
i.	Must support variety of operating systems including: Windows Server, Red Hat Enterprise Linux, SUSE Linux Enterprise Server etc.		
ii.	Service shall be available online, on-demand and dynamically scalable up or down per request for service from the HLL's authorized team member(s) with two factor authentications via the SSL through a web browser		
iii.	Service shall provide auto-scalable, redundant, dynamic computing capabilities of virtual machines		
iv.	Should support auto scaling of the compute service on the basis of CPU utilization of the Instance		
v.	Should support block storage and temporary block storage (to store Information that changes frequently, such as buffers, caches, scratch data, and other temporary content)		
vi.	CSP should offer tools to monitor VM up/down status and resource utilization such as RAM, CPU, Disk, IOPS and network		
vii.	Virtual Machines offered should be with the latest generation processor offered by the processor OEM in the last two years.		
viii.	Physical core to vCPU ratio should be 1:2 for all the proposed Virtual Machines		
ix.	CSP should offer an ability to automatically increase or scale- out the number of Instances/VMs during demand spikes to maintain performance (i.e., 'scale-out'), as well as an ability to automatically decrease the number of deployed Instances if the demand drops		
x.	Required Operating System should be offered along with the Virtual Machines and should support both BYOL (Bring your own license) as well as PAYG (Pay as you go). The OS offered should come with continuous updates and upgrades for the entire contract duration.		

xi.	Cloud service must offer self-service provisioning of multiple instances concurrently either through a programmatic interface (API/CLI/Infra as code) or through a management console		
xii.	Cloud Service should offer Pay-as-You-Go Pricing as well as reserved option of pricing providing better pricing discounts if the customer commits to a workload		
xiii.	In the Pricing / Reserved Capacity model the Cloud service should offer flexibility of changing the instances families/types		
2.	**Block or Instance Storage**		
i.	CSP should offer persistent block level storage volumes for use with compute instances		
ii.	CSP shall offer Storage Service which shall provide scalable, redundant and dynamic storage up or down per request for service from the end users		
iii.	For all volumes pertaining to production VMs, Solid State Device (SSD) based Block Storage should be offered with support of minimum 7500 IOPS to maximum 10000 IOPS with 125 MB/S – 750 MS/s throughput.		
iv.	For the proposed Block Storage, CSP should offer the capability to increase the size of an existing block storage volume without having to provision a new volume and copy/move the data.		
v.	Block Storage with minimum monthly uptime of 99.99% or higher (as published in the CSP’s Public Portal)		
vi.	Cloud storage service should support the needs of I/O-intensive workloads, particularly database workloads that are sensitive to storage performance and consistency in random access I/O throughput.		
vii.	Cloud service should support encryption of data on volumes, disk I/O, and snapshots using industry standard AES-256 cryptographic algorithm.		
viii.	Cloud service should support point-in-time snapshots. These snapshots should be incremental in nature		
ix.	Block Storage should be one continuous disk and the CSP should have capability to add more storage to the same. If the CSP doesn’t have any particular variant of the Storage available they need to select the next better version.		

3.	**Object Storage**		
i.	CSP should offer secure, durable, highly scalable object storage for storing and retrieving any amount of data from the web.		
ii.	CSP should support an extremely low-cost storage for archival.		
iii.	Cloud service should support encryption for data at rest using 256-bit Advanced Encryption Standard (AES-256) encryption to encrypt your data		
iv.	Cloud Service should offer geographical redundant object storage with copies of data stored in 3 different physical location (MeitY Empaneled)		
v.	Cloud service should support encryption using customer provided keys. These keys should be used to manage both the encryption, as data is written to disks, and decryption, when data is accessed		
vi.	Cloud Service should support managing an object's lifecycle by using a lifecycle configuration, which defines how objects are managed during their lifetime, from creation/initial storage to deletion		
vii.	Cloud service should be able to send notifications when certain events happen at the object level (addition/deletion).		
viii.	Cloud Service should support versioning, where multiple versions of an object can be kept in one folder/bucket. Versioning protects against unintended overwrites and deletions.		
ix.	Cloud service should support flexible access-control policies to manage permissions for objects.		
x.	Cloud service should be able to provide audit logs on storage buckets including details about a single access request, such as the requester, bucket name, request time, request action, response status, and error code.		
xi.	Cloud service should allow uploading a single object as a set of parts where each part is a contiguous portion of the object's data and these object parts can be uploaded independently and in any order.		
xii.	Cloud service should support read-after write consistency for PUT operations for new objects		
xiii.	Object storage should have integration with HSM to provide inherent capability of encryption		

xiv.	CSP should offer managed cloud native Object storage service with automatic replication to 3 or more MeitY empaneled Data centers		
xv.	CSP shall offer different tiers of managed cloud native Object storage services and the CSP should have the capability of performing intelligent and automatic migration of data between various classes/tiers of storage based on the usage		
4.	**File Storage**		
i.	CSP should offer a simple scalable file storage service to use with compute instances in the cloud.		
ii.	Cloud service should offer SSD backed storage media to provide the throughput, IOPS, and low latency needed for a broad range of workloads.		
iii.	Cloud service should support petabyte-scale file systems and allow thousands of concurrent NFS connections.		
iv.	Cloud service should support consistent low latency Performance between 5-15 MS at any scale.		
v.	Cloud service should support scalable IOPS and Throughput performance at any scale.		
vi.	Cloud service should support thousands of instances so that many users can access and share a common data source.		
vii.	Cloud service should automatically scale up or down as files are added or removed without disrupting applications.		
viii.	Cloud service should be highly durable - file system object (i.e. directory, file, and link) should be redundantly stored across multiple data center.		
ix.	Cloud service should support read after write consistency (each read and write operation is guaranteed to return the most recent version of the data).		
5.	**Fully Managed* Relational Database Services**		
i.	The CSP should provide/support of relational database services MySQL, PostGreSQL, Maria DB, MS SQL, Oracle Std DB as a native cloud service enabling handling of routine database tasks such as provisioning, read replica, synchronous replication to secondary instance, patching, backup, recovery, failure detection and automatic switch over on same DNS endpoint, and repair etc.		

ii.	Support synchronous replication and automatic failover of a primary database to a standby database copy in a separate physical datacentre to improve data redundancy		
iii.	Offer encryption of data 'at-rest' and 'in-transit'		
iv.	Support the creation of on-demand (i.e., user-initiated) point-in-time copies (snapshots) and the restoration of a database instance using one of these copies		
v.	Cloud provider should offer a service that makes it easy to setup, operate, and scale a relational database in the cloud.		
vi.	Cloud service should support the last two major releases of MySQL as a database engine as a cloud native CSP managed service		
vii.	Cloud service should support all the editions (Web, Standard, Enterprise) of SQL Server 2012, 2017, 2019 or higher versions as a database engine as a cloud native CSP managed service		
viii.	Cloud service should support the last two major releases of PostgreSQL as a cloud native CSP managed service		
6.	**No-SQL Database**		
i.	**Scalable, fast, and flexible NoSQL database service** CSP should offer a fast and flexible NoSQL database service for applications that need consistent, single digit millisecond latency at any scale.		
ii.	**Replication** Cloud service should support automatic replication of data across multiple physical datacenters in a region to provide high availability and data durability		
iii.	**Performance/Latency** Cloud service should support single-digit milliseconds latencies at any scale.		
iv.	**Key-value Data Model support** Cloud service should support key value data structure wheretheprimarykeyistheonlyrequiredattributeforitemsinat ableanduniquelyidentifieseach item.		
v.	**Document Data Model with JSON support** Cloud service should support storing, querying and updating JSON documents.		
vi.	**Tenable Scaling** Cloud service should support seamless throughput and storages calling.		

vii.	**Secondary Indexes** Cloud service should support secondary indexes. Secondary indexes are indexes that contain hash or hash- and-range keys that can be different from the keys in the table on which the index is based.		
viii.	**Streams** Cloud service should support streams .Stream is an ordered flow of information about changes to items.		
ix.	**Database triggers** Cloud Service should support database triggers-pieces of code that quickly and automatically respond to data modification in the tables.		
x.	**Strong consistency, Atomic counters** Cloud service should support strong consistency forreadoperationstomakesureusersarealwaysreadingthelatestvalues.		
xi.	**Integrated Monitoring** Cloud service should support monitoring of request throughput and latency for database tables, among other metrics.		
xii.	**Integration with data warehouse** Cloud service should support integration with a data warehouse for advanced business intelligence capabilities.		
xiii.	**Hadoop Integration** Cloud service should support integration with a Hadoop framework to perform complex analytics on large datasets		
xiv.	CSP should offer Memory DB Redis/ Elastic Cache services for Database		
xv.	CSP should offer for Graph DB services for Database		
7.	**Virtual Network / Networking / Hybrid Connectivity requirement**		
i.	Provide a virtual local area network (LAN) infrastructure and static IP addresses of non-internet routable addresses.		
ii.	Ability to deploy VMs in multiple security zones, as required for the project, defined by network isolation layers.		
iii.	Provide private connectivity between the HLL's network and CSP's Data Centre facilities (Direct Connection/Express Route)		

iv.	Provide infrastructure that allows to provide an external ipv6 address termination for applications hosted on Cloud.		
v.	The datacentre and disaster recovery datacentre facilities (where applicable) should support connection to the wide area network through high bandwidth links of appropriate capacity to take care of the needs of various types of user entities. Provision has to be made for segregation of access path among various user categories.		
vi.	CSP shall have the capability to provide adequate bandwidth between Primary Data Centre and Disaster Recovery Centre for data replication purpose.		
vii.	Support network level redundancy through MPLS links from two different service providers, alternate routing paths facilitated at ISP backbone (MPLS), redundant network devices etc.		
viii.	**Multiple network interface/instance** Cloud service should be able to support multiple (primary and additional) network interfaces		
ix.	**Multiple IP addresses/instance** Cloud service should be able to support multiple IP addresses per instance. Use cases include hosting multiple websites on a single server and network appliances (such as load balancers) that have multiple private IP addresses for each network interface		
x.	**Ability to move network interfaces and IPs between instances** Cloud service should support the ability to reserve static IP and attach it to an instance, detach it from an instance and attach it to another instance.		
xi.	**Enhanced networking support** Cloud service should support capabilities such as single root I/O virtualization or other equivalent capability that offloads virtual network processing to hardware for higher performance (packets per second), lower latency, and lower jitter.		
xii.	**Network traffic logging** - Log traffic flows at network interfaces (flow log) Cloud service should support capturing information about the IP traffic going to and from network interfaces.		
xiii.	**Auto-assigned public IP addresses** Cloud service should be able to automatically assign a public IP to the instances		

xiv.	**IP Protocol support** Cloud service should be able to support multiple IP protocols, including TCP, UDP, and ICMP protocols.		
xv.	**Use any network CIDR, including RFC 1918** Cloud service should be able to support IP address ranges specified in RFC 1918 as well as publicly routable CIDR blocks.		
xvi.	**Static public IP addresses** CSP must support IP addresses associated with a customer account, not a particular instance. The IP address should remain associated with the account until released explicitly.		
xvii.	**Auto-created default virtual private network** Cloud service should be able to create a default private network and subnet with instances launching into a default subnet receiving a public IP address and a private IP address.		
xviii.	**Subnets within private network** Customer should be able to create one or more subnets within private network with a single Classless Inter-Domain Routing (CIDR) block		
xix.	**Ingress filtering (Security groups)** Cloud service should support adding or removing rules applicable to inbound traffic (ingress) to instances		
xx.	**Endpoint Services** CSP Should support Endpoint services for accessing various resources from internal cloud network		
8.	**Container Service**		
i.	Share and deploy container software, publicly or privately		
ii.	Manage containers with Kubernetes.		
iii.	Should provide private or public dedicated container registry to store , deploy and share the containers		
iv.	Should also provide platform to run container without managing servers		
v.	Should also help to containerize and migrate existing application		
vi.	Cloud service should support deployment of Docker container with orchestration (Kubernetes/any native orchestration System)		

9.	**DevOps**		
i.	Automatically build, test, distribute, deploy and monitor iOS, Android, Windows and mac OS apps—all in one place		
ii.	Developers can regularly merge their code changes into a central repository, after which automated builds and tests are run.		
iii.	Must provide fully managed service to implement end to end CI CD (Continuous Integration & Continuous Delivery) pipeline		
iv.	Should securely store and version application's source code and automatically build, test, and deploy the application		
v.	Cloud Service Provider should offer a **fully managed*** service to analyse and debug applications		
vi.	The manage service to analyse and debug applications should have Filtering capability and interactive capability to interpret trace data		
vii.	Cloud Service Provider should offer a Cloud based IDE service to collaborate with the developers in real time		
viii.	Cloud Service Provider should offer a managed source control service to store code in Private Git Repositories		
10.	**Analytics service**		
i.	Should provide **fully managed*** and native service platform for • Interactive Analytics • Big Data Processing • Real time analytics • Operational Analytics • Data Visualization & Visual Data Preparation • Real Time Data Movement • Predictive analytics and Machine Learning		
ii.	CSP should offer an analytics service which should be server less - No need to provision or maintain any servers. There is no software or runtime to install, maintain, or administer		
iii.	CSP should offer service to build custom, real-time applications that process data streams using popular stream processing frameworks		

iv.	CSP should offer an analytics service to process data streams in real time with SQL without having to learn new programming languages or processing frameworks		
v.	CSP should offer managed Business Intelligence (BI) service with an ability to embed dashboards to applications		
vi.	CSP should offer business analytics service that makes it easy for all employees within an organization to build visualizations, perform ad-hoc analysis, and quickly get business insights from their data, anytime, on any device.		
vii.	BI service should support data ingestion from multiple data sources and multiple databases engines		
viii.	Cloud service should support provisioning of on demand Hadoop cluster and schedule map reduce and spark job		
ix.	Cloud service should support provisioning of Manages key Value Pair Search Services (Elastic Search/ Cloud Search)		
x.	Cloud service should support provisioning of Data Pipeline (Extract Transformation Loading Tool)		
11.	**Management and Governance**		
i.	CSP should have multi-account management and governance service with ability to consolidate payments from multiple accounts and ability to share resources across accounts		
ii.	CSP should have capability to create and manage resources with templates		
iii.	CSP should have a managed service to manage multi-account environments and also offer blueprints based on cloud provider's best practices		
iv.	CSP should have capability to enforce organization level security compliance and governance		
v.	Cloud service should trigger events and alerts on non-conformance on defined organization level governance and should have capability prevent the configuration changes.		
vi.	CSP should offer a service to create a collection of related resources and provision them in an orderly and predictable fashion using a template		

vii.	Cloud service should use a template, a JSON-format, text-based file that describes all the resources required for an application		
viii.	CSP should have a management service to enable auditing, security monitoring, and operational troubleshooting by tracking user activity and API usage.		
ix.	CSP should offer a monitoring service for cloud resources and the applications they run on cloud. The service should collect and track metrics, collect and monitor log files, and set alarms.		
x.	CSP should offer a managed service for resource inventory, configuration history and change notifications		
xi.	The Cloud service should supports SQL based reporting		
xii.	CSP should provide guidelines for provisioning, configuring, and continuously monitoring		
xiii.	Send real-time notifications for resource configuration and compliance changes.		
xiv.	Supports automatic remediation of noncompliant resources.		
xv.	CSP should offer a managed service for Cloud Infrastructure Management.		
xvi.	Cloud Infrastructure Management service should have Ability to distribute 3rd party ISV agents		
xvii.	Ability to deploy OS and patches across a large group of resources		
xviii.	Ability to schedule maintenance windows for disruptive tasks		
xix.	Automates IT resource operations and management		
xx.	Easy GUI based management of Windows and Linux instances at scale		
xxi.	CSP should offer a Tool to review cloud workloads against architectural best practices		
xxii.	CSP should have a service to continuously audit and assess the overall compliance of the cloud resources.		
12.	**Security**		
i.	CSP must provide native service for security like Identity & access management, manage user access and encryption keys, Single sign on service for cloud and a Centralize Governance and Compliance Management		

ii.	Proposed Hardware Security Module (HSM) should be a managed service of same cloud service provider for ease of integrations, manageability and deeper integrations with rest of the services. CSP should support FIPS 140-2 Level 3 for the storage of encryption keys SSL certificates etc. as managed service		
iii.	Security service should be capable to provide Protection for Layer 3 and Layer 4 DDoS attacks that target to web applications. Shall provide DDoS for 200 resources with public ip protected.		
iv.	OS and Application patch should be done automatically as per patch schedule and maintenance window. It should also provide dashboard to see the list of non-compliant resource		
v.	System should be agent less which can detect threat while scanning the network, DNS and API logs and able to detect attack reconnaissance, brute force attack, credentials compromise, Bitcoin or Tor Domain Request, Port Sweep Attack, Spam Bot, DNS Data Exfiltration etc.		
vi.	CSP should offer a service to support stateless and stateful firewall rules to control port, IP and Domain bases rules. Apart from it should support custom rules definitions to control additional traffic types.		
vii.	Firewall must be able to provide intrusion prevention support along with capability to provide protection from malicious domain, domain hosting malware, domains which looks legitimate but are compromised and may host botnets etc.		
viii.	CSP should offer a native security service to filter malicious web traffic through a Web Application Firewall		
ix.	CSP should offer Distributed Denial of Service (DDoS) protection service for L3/L4 attacks.		
x.	CSP should offer Managed Threat Detection Service that uses intelligence, machine learning and advanced features to continuously monitors for malicious activity and unauthorized behaviour to monitor the cloud resources.		
xi.	Proposed CSP cloud native IAM services should include support for granting users IAM roles at the organization, folder, and project levels.		

13.	**Cloud Advisor**		
i.	The CSP should offer recommendations around resource configurations and security the customer can make to optimize their financial spend with the provider.		
Ii	The CSP should offer a service acts like a customized cloud expert and helps provision resources by following best practices.		
14.	**SAP Solution Requirements**		
i.	CSP should provide an SAP-certified cloud infrastructure for running SAP HANA. CSP should have more than 100+ instances certified by SAP.		
ii.	For HANA Data Volumes of all proposed VMs, Premium SSD based Block Storage (SSD) should be offered to provide a minimum of 9000 IOPS and throughput of 1500 MB/s for 3.6 TB of persistence storage For HANA log Volumes of all proposed VMs, Premium SSD based Block Storage (SSD) should be offered to provide a minimum of 3000 IOPS and throughput minimum of 500 MB/s for 512 GiB of persistence storage The above requirement should be met by both compute instance and storage		
iii.	Bidder should provide clustering solution as active-active combined HA/DR configuration for SAP application and using synchronous HANA system replication for database. The HA solution should provide the automated failover functionality within the nodes in case of: • Hardware failure in the box • OS failure • Network / Link failure • Database Server failure • Failover of Active Database instance from Primary node to Secondary Node and vice-versa The cluster configuration should meet the application availability with RTO of 15 mins and RPO ~0 for HANA DB		
iv.	Solution should support automatically scale up or scale down of instances based on SAP work process utilization without impacting any end user connectivity.		

v.	CSP shall provide Intel x86 certified instances for the proposed solution		
vi.	Storage for SAP - CSP should provide all the required storage options for setting up database and SAP application without any minimum restrictions.		
vii.	CSP should provide a Cloud Native Service/ Fully managed service to automatically install, setup and configure SAP system along with HANA database in standalone and high availability configuration. The Cloud native service should facilitate automatic deployment of SAP System/Solution “End to End” and not limiting to automatic deployment of Infrastructure as a service alone. This service should be available from the User Interface console/portal of the respective Cloud Service Provider		
viii	SAP Server Auto scaling - CSP should provide auto scaling solution for SAP system based on SAP architecture (i.e.: based on availability of SAP work processes) without any disturbances during scale up or scale down mechanism. The auto scaling mechanism should not be based on CPU or Memory utilization alone and it should be performed on the “availability of SAP work processes”.		
ix.	HANA Database Predictive monitoring - CSP should be able to provide a cloud native automated predictive monitoring solution based on AI/ML platform to monitor SAP HANA database in real time. The solution should also use the historical data to detect anomalies and provide insights through a centralized dashboard for all the HANA systems in the landscape. The predictive monitoring solution should be able to detect issues even before they occur and issue customized notifications/alerts to the administrator to prevent unplanned downtime rather than providing a regular monitoring dashboard. This service should be available from the User Interface console/portal of the respective Cloud Service Provider		

FORM A7: Format for NEFT Mandate Form

Electronic Payment Mandate Form

(Mandate for receiving payments through NEFT HLL Lifecare Ltd)

1) Vendor/Contractor Name :

2) Vendor/Contractor Address :

3) Vendor Code :

4) Permanent Account Number(PAN) :

5) Particulars of Bank Account

Form A8

FORM A8: Pre-Bid Questionnaire

Sl No.	Reference Clause	Page No	Description	Bidder's Query	HLL Reply

Date:	Authorized Representative Signature:
Place:	Name:
Designation:	
Company Name:	
Seal of Company	

Form A9

Form A9- FORMAT OF BID SECURITY DECLARATION FROM BIDDERS IN LIEU OF EMD

(On Bidders Letter head)

I / We, the authorized signatory of M/s ...., participating in the subject tender No. .... for the item / job of.., do hereby declare:

(i) That I / we have availed the benefit of waiver of EMD while submitting our offer against the subject Tender and no EMD being deposited for the said tender.

(ii) That in the event we withdraw / modify our bid during the period of validity OR I/we fail to execute formal contract agreement within the given timeline OR I/we fail to submit a Performance Security within the given timeline OR I/we commit any breach of Tender Conditions / Contract which attracts penal action of forfeiture of EMD and I/we will be suspended from being eligible for bidding /award of all future contract(s) of HLL Lifecare Limited for a period of one year from the date of committing such breach.

Date:	Authorized Representative Signature:
Place:	Name:
Designation:	
Company Name:	
Seal of Company	

Form A10

FORM A10: Format for Price Bid

Price Bid for “Installation, Configuration and Maintenance of Cloud Based Infrastructure for hosting the SAP Applications of HLL”

(Please submit in a separate Envelope. The Technical Bid must not contain any price information else the bidder will be liable to be disqualified.)

(TOTAL AMOUNT IN WORDS: - INR ....
....)

Authorized Signatory with Seal
Date:
Place:

Notes:-
1. The prices should be quoted in INR only

2. GST should be mentioned in the separate column as provided in the format

3. Providing Price bid other than this format may lead to rejection of the bid.