RFP FOR ENGAGEMENT OF MANAGED SERVICE PROVIDER FOR CLOUD BASED DC & DR FOR LIFTING & SHIFTING E-KOSH APPLICATION

Directorate of Treasury, Account & Pension, Government of Chhattisgarh,
1st Floor, ‘A’ Block, Indravati Bhawan, Nawa Raipur Atal Nagar,
Chhattisgarh – 492101

Issued On- 10/06/2024

छत्तीसगढ़ शासन
सत्यमेव जयते

Disclaimer

This Request for Proposal (“RFP”) is issued by the Directorate, Treasury, Accounts & Pension, and Government of Chhattisgarh. Whilst the information in this RFP has been prepared in good faith, it is not and does not purport to be comprehensive or to have been in dependently verified. Neither Directorate, Treasury, Accounts & Pension, Government of Chhattisgarh, nor any of its officers or employees, neither any of the advisers nor consultants accept any liability or responsibility for the accuracy, reasonableness or completeness of, or for any errors, omissions or misstatements, negligent or otherwise, relating to the proposed project, or makes any representation or warranty, express or implied, with respect to the information contained in this RFP or on which this RFP is based or with respect to any written or oral information made or to be made available to any of the recipients or their professional advisers and, so far as permitted by law and except in the case of fraudulent misrepresentation by the party concerned, and liability therefore is hereby expressly disclaimed.

The information contained in this RFP is selective and is subject to updating, expansion, revision and amendment at the sole discretion of Directorate Treasury, Accounts & Pension, (DTAP) Government of Chhattisgarh. It does not, and does not purport to, contain all the information that a recipient may require for the purposes for deciding for participation in this process. Neither Directorate, Directorate Treasury, Accounts & Pension, (DTAP), Government of Chhattisgarh nor any of its officers, employees nor any of its advisors nor consultants undertakes to provide any Party with access to any additional information or to update the information in this RFP or to correct any inaccuracies therein which may become apparent. Each Party must conduct its own analysis of the information contained in this RFP, to correct any inaccuracies therein and is advised to carry out its own investigation into the proposed project, the regulatory regime which applies thereto and by and all matters pertinent to the project and to seek its own professional advice on the legal, financial and regulatory consequences of entering into any agreement or arrangement relating to the project.

Time and Quality is of essence. The Authority reserves the right to go ahead with the bid in case of single bidder. It is also not bound to accept the lowest financial offer and may negotiate with the most technically qualified bidder.

This RFP includes certain statements, estimates, projections, targets, and forecasts with respect to the project. Such statements estimate, projections, targets and forecasts reflect various assumptions made by the management, officers and employees of Directorate, Directorate Treasury, Accounts & Pension, (DTAP), Government of Chhattisgarh, which assumptions (and the base information on which they are made) may or may not prove to be correct. No representation or warranty is given as to the reasonableness of forecasts or the assumptions on which they may be based and nothing in this RFP is, or should be relied on as, a promise, representation, or warranty.

Proprietary Notice:

This document contains confidential information of Directorate, Treasury, Accounts & Pension, and Government of Chhattisgarh which is provided for the sole purpose of permitting the recipient to make a proposal. In consideration of receipt of this document, the recipient agrees to maintain such information in confidence and to not reproduce or otherwise disclose this information to any person outside the group directly responsible for evaluation of its contents, except that there is no obligation to maintain the confidentiality of any information which was known to the recipient prior to receipt of such information from Directorate, Treasury, Accounts & Pension, Government of Chhattisgarh or becomes publicly known through no fault of recipient, from Directorate, Treasury, Accounts & Pension, Government of Chhattisgarh or is received without obligation of confidentiality from a third party owing no obligation of confidentiality to Directorate, Treasury, Accounts & Pension, Government of Chhattisgarh.

Table of Contents

1. INTRODUCTION

The objective of this Request for Proposal (RFP) is to allow the Directorate of Treasuries, Accounts &Pension (DTAP) to acquire cloud services from a MeitY empanelled Cloud Service Providers (CSPs) for hosting the Integrated Financial Management Information System (IFMIS) application. This is in line with the Cloud First policy of MeitY under which all the departments are required to assess and adopt cloud computing for their current as well as new applications. The RFP also outlines the key responsibilities of the DTAP and the Managed Service Providers (MSP) through Meity-empanelled CSP during the procurement of cloud services.

The proposed cloud solution offered by the MSP must be scalable, extensible, highly configurable, secure and very responsive and must support integration and interfacing with other software's and solutions (existing legacy or acquired in future), developed or used by the NIC or state departments or its Directorates/associate institutions and/or other stakeholders. The proposed deployment plan for the IFMIS solution includes four environments:

a. Production,
b. Development/Testing,
c. Staging, and
d. Disaster Recovery.

The Directorate of Treasuries, Accounts & Pension also hopes to achieve cost savings through an "OPEX"/ "pay-per-use" model, where DTAP only pays for the resources, it uses.

1.1 Request for Proposal (RFP)

Sealed tenders are invited from eligible, reputed, qualified Managed Service Providers (MSPs) firms with sound technical and financial capabilities for lifting & shifting the e-Kosh (IFMIS) application and providing cloud services with the establishment and operation of related outsourced process operating units as detailed out in the scope of work section of this RFP document.

The intent of this RFP is to invite proposals from the agencies/firms/companies (also referred to as 'bidders') to enable the DTAP to select Managed Service Providers (MSPs).

This invitation to bid is open to all bidders meeting the pre-qualification criteria as mentioned in Section Pre-Qualification Evaluation of this RFP document.

1.2 Project Background

Directorate of Treasuries, Accounts & Pension (DTAP) is a directorate of the State Government that operates under the Finance Department, Government of Chhattisgarh. The department is responsible for managing all financial transactions made by the State Government through the Integrated Financial Management Information System (IFMIS), also termed as e-Kosh application. The IFMIS is managed by the National Informatics Centre (NIC)and is overseen by the DTAP.

IFMIS application (e-Kosh and related applications) of Govt. of Chhattisgarh is used by different departments, and their offices to carry out several functions across the lifecycle of Public Financial Management (PFM). The current set of applications have been developed over a period of time. National Informatics Center (NIC) Chhattisgarh has developed different modules/applications of IFMIS under the guidance of Directorate of Treasury, Accounts & Pension and the Finance Department, Govt. of Chhattisgarh.

E-Kosh application is of a high importance and critical for day-to-day state financial activities and operations, the application must be on a robust, highly available, secured and scalable and easy manageable environment. It is well expected that bidder is aware about the functions, volume and criticality of the application. For improved facilities management and standardized platform, department looking to upgrade the infrastructure platform and migrate the application.

1.3 EXISTING SETUP

Currently the whole Infrastructure is deployed at NIC, Data Center, Mahanadi Bhawan, Naya Raipur Chhattisgarh. Further, Data Recovery (near DR) has been setup in CHiPS.

At Data Center (DC), we are Using Blade Servers for Deployment of Database, Application, and Integrations. We are using San Storage of DELL EMC ME4024 of 50 TB(Approx) Space.

Below is the Summarized View of the Infrastructure:

- Database Platform: Intel Xeon CPU E5-46200 X86 platform - Estimated 32 Cores
- Database Version: Oracle Database Enterprise Edition 19c (19.17.0.0.0)
- Database Storage: ~ 10 TB
- Operating System: Windows Server 2012 R2 Standard
- Application Platform: Intel Xeon CPU E5-46200 X86 platform VMs- Estimated 44 Cores
- Front end: .net V4.0, Node js v18.12.1, Tomcat 9.0

For availability and data protection, existing approach is based on database backup and recovery, also the system has been configured for operating system cluster.

Serial No.	Server	Cores	RAM	Storage
1	DB-Server-Node-1 (VM)	32	300 GB	10 TB
2	App-Server-1 (VM)	32 (75)	Dynamic (8-64 GB)	830GB
3	App-Server-2 (VM)	16 (77)	32GB	700GB
4	App-Server-3 +Sftp-Server-1 (VM)	8 (76)	8GB	130GB
5	App-Server-4 (VM)	8 (85)	8GB	400GB
6	App-Server-5 (VM)	8 (89)	8GB	150GB
7	App-Server-6 (VM)	8 (91)	8GB	350GB
8	App-Server-7 (VM)	8 (94)	8GB	150GB
9	App-Server-8 (VM)	8 (101)	16GB	300GB
10	App-Server-9 (VM)	8(90)	8GB	150GB
11	Domain-Server (One of the physical server)	32	512 GB	300 GB
12	Virtualization-Server	32x4	521x4	50 TB
13	Sftp-Server-2 (VM)	4	4 GB	10 GB
14	Test-DB-Server (VM)	32	300 GB	10 TB
15	Test-App-Server (VM)	8	8 GB	200 GB
16	DR-DB (at SDC) (VM)	32	300 GB	3 TB
17	SAN details—DELL EMC HP 3PAR 7200 x 2			50 TB 10TB
18	Existing OS Software Licenses – MS Windows Server 2012 Standard			
19	DB-Server (SQL Server) Bug track (VM)	8	32 GB	250 GB
20	DB-Server (SQL Server) Budget Allocation (VM)	8	8 GB	150 GB
21	App-Server-10 (VM)	1	2 GB	100 GB

Serial No.	Server	Cores	RAM	Storage
22	OEM Deployment (VM)	8	64 GB	100 GB
23	DB-Server (Postgresql 12) (VM)	8	16 GB	250 GB

Serial No.	Name	No. of License (For database)
1	Oracle Active Data Guard - Processor Perpetual	04
2	Oracle Diagnostics Pack - Processor Perpetual	04
3	Oracle Tuning Pack - Processor Perpetual	04
4	Oracle Database Enterprise Edition - Processor Perpetual	04

Serial No	Name	Specification
1	NGFW Firewall	Hardware Firewall deployed
2	Leased Line	BSNL MPLS LEASE LINE

2. ***INSTRUCTIONS TO BIDDERS***

2.1 General Instruction to Bidders

While every effort has been made to provide comprehensive and accurate background information and requirements and specifications, Bidders must form their own conclusions about the solution needed to meet the requirements. Bidders and recipients of this RFP may wish to consult their own legal advisers in relation to this RFP.

All information supplied by Bidders may be treated as contractually binding on the Bidders, on successful award of the assignment by the DTAP based on this RFP.

No commitment of any kind, contractual or otherwise shall exist unless and until a formal written contract has been executed by or on behalf of the DTAP. Any notification of preferred Bidder status by the DTAP shall not give rise to any enforceable rights by the Bidder. The DTAP may cancel this public procurement at any time prior to a formal written contract being executed by or on behalf of the DTAP.

This RFP supersedes and replaces any previous public documentation & communications, and Bidders should place no reliance on such communications.

2.2 Bid Fact Sheet

The bidders should be provided with this Bid Fact Sheet comprising of important factual data on the tender.

No.	Information	Details
Introduction		
1.	Project Name	RFP for selection of Managed Service Provider (MSP) for hosting, commissioning, data migration and O&M of e-Kosh application on cloud environment.
2.	Tender Published by	Directorate of Treasury, Accounts & Pension (DTAP), Finance Department (GoCG)
3.	Tender No.	1127 Dt. 10/06/2024
e-Tendering Portal		
4.	e-Tendering Website	https://eproc.cgstate.gov.in
5.	e-Tendering Support	For latest details on the support mechanism, the bidder may visit e-Tendering Portal 1800 419 9140 (Toll free) helpdesk.cgeproc@mjunction.in
Tender Fees and Earnest Money Deposit		
6.	Tender Fee	Rs. 20,000/- (Twenty Thousand Only) to be paid through DD only
7.	Earnest Money Deposit	Rs. 10,00,000/- (Rupees Ten lakh Only) in the form of DD or through Challan in the head 8443-103.
8.	Submission of EMD and Power of Attorney (physical hard copy submission)	Demand Draft of EMD and Power of Attorney shall be submitted in the format provided in the Annexure-I of this RFP. Scanned Copy of DD of EMD or Challan in the head 8443-103 and Power of Attorney also needs to be uploaded on e-Procurement portal under a separate cover.

No.	Information	Details
9.	Address for Submission of EMD and Power of Attorney (physical hard copy submission)	Directorate Of Treasury, Account & Pension, Government of Chhattisgarh, 1st Floor, A Block, Indravati Bhawan, Nawa Raipur Atal Nagar, Chhattisgarh – 492101
RFP Availability and Mode of Submission		
10.	Availability of RFP Documents	RFP document and amendments can be downloaded from the e-Tendering Portal and e-Kosh online portal (https://ekoshonline.cg.nic.in/)
11.	Mode of submission of RFP	As mentioned in sub-section titled 'Contents of Covers'. The detailed information regarding the submission can be obtained from e-Tendering Portal. Bidders are required to submit Original DD of Tender fees and EMD prior to 12.00 pm on the last date of bid submission. The Original DD/Challan shall be submitted to address mentioned above in point no. 9 by any of the mentioned means Book Post/Speed Post/by hand. The other parts of proposal, Bid Submission will be online through e-Tendering Portal only. Please note that only online bids will be considered for evaluation of offers.
12.	Bid Validity Period	12 months from the last date and time of submission.
13.	Currency	Currency in which the Bidders may quote the price and will receive payment is – Indian Rupees Only (INR)
14.	Language of Bid Submission	Proposals should be submitted in English only
Communication Details		
15.	Communication Address	All communications, including proposal documents should be addressed to: The Director Directorate of Treasury, Account & Pension, Government of Chhattisgarh, 1st Floor, A Block, Indravati Bhawan, Nawa Raipur Atal Nagar, Chhattisgarh – 492101 Tel.: 0771-2331305 dir.treasury.cg@gov.in
Important Dates		
16.	Start date of issuance of RFP document	11 June, 2024 at 02.00 pm
17.	Last date and time for RFP Submission	01 July, 2024 at 12:00 am
18.	Date and time of opening of bid	01 June 2024, 01:00 pm
19.	Method of Selection	The method of selection is: Lowest Cost Based

No.	Information	Details
		Selection (LCBS) – L1 selection
20.	Performance Guarantee	Performance Guarantee should be equivalent to the 3% of Total Contract Value. The Performance Guarantee should be issued by the nationalized/scheduled bank having an operational branch in the State of Chhattisgarh.

2.3 RFP Document Availability

a) The RFP documents have been made available for download from e-Procurement Portal and e-Kosh online portal.

b) The Bidders shall submit, along with their Bids, a non-refundable Tender Fee (refer Bid Fact Sheet for details). The payment shall be acceptable in following forms and payment in any other form will not be accepted:

(i) On e-Procurement System during bid submission process Bid submission fees of Rs. 311/- should be deposited online on CHiPS account through e-procurement website https://eproc.cgstate.gov.in

or

(ii) RFP document fees receipt should be submitted along with the bidder’s proposal.

c) Proposals received without or with inadequate non-refundable RFP Document fees shall be rejected.

2.4 Changes in the Bidding Document

a) At any time, prior to the deadline for submission of Bids, the procuring entity may for any reason, whether on its own initiative or as a result of a request for clarification by a bidder, modify the bidding documents by issuing an addendum.

b) Any bidder, who has submitted his Bid in response to the original invitation, shall have the opportunity to modify or re-submit it, as the case may be, within the period of time originally allotted or such extended time as may be allowed for submission of Bids, when changes are made to the bidding document by the procuring entity: Provided that the Bid last submitted or the Bid as modified by the bidder shall be considered for evaluation.

2.5 Directorate of Treasury, Accounts & Pension (DTAP) rights to terminate the tender

a) DTAP reserves the right to accept or reject any proposal, and to annul the bidding process and reject all proposals at any time prior to award of agreement, 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 actions taken by DTAP.

b) DTAP makes no commitments, express or implied, that this process will result in a business transaction with anyone.

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

2.6 EMD (Earnest Money Deposit)

a) The Bidders shall submit, along with their bids, a Bid security/ Earnest Money Deposit (EMD) (amount mentioned in fact sheet) offline at DTAP as per the details mentioned in the factsheet of this RFP.

b) EMD of all unsuccessful Bidders would be refunded by the DTAP after the Bidder being notified as being unsuccessful. The EMD, for the amount mentioned above, of successful Bidder would be returned upon submission of Performance Bank Guarantee. as per the format provided in the RFP.

c) The EMD amount is interest free and will be refundable to the unsuccessful Bidders without any accrued interest on it.

d) Proposals do not accompany with the EMD or containing EMD with infirmity(ies) (relating to the amount or validity period etc.), mentioned above, shall be summarily rejected.

e) The EMD may be forfeited in the event of:

(i) A Bidder withdrawing its bid during the period of bid validity.

(ii) A successful Bidder fails to sign the subsequent contract in accordance with this RFP.

(iii) The Bidder being found to have indulged in any suppression of facts, furnishing of fraudulent statement, misconduct, or other dishonest or other ethically improper activity, in relation to this RFP.

(iv) A Proposal contains deviations (except when provided in conformity with the RFP) conditional offers and partial offers.

2.7 Bidder's Authorized Signatory

The bid shall be uploaded using digital signature certificate of the authorized signatory of the bidder online at e-Procurement portal.

2.8 Interlineations in Bids

The bid shall contain no interlineations, erasures or overwriting except as necessary to correct errors made by the bidder, in which case such corrections shall be initialed by the person or persons signing the bid.

2.9 Bid Preparation and Submission Instructions

a) Proposals must be direct, concise, and complete. All information not directly relevant to this RFP should be omitted. DTAP will evaluate bidder's proposal based on its clarity and the directness of its response to the requirements of the project as outlined in this RFP.

b) Bidders shall furnish the required information on their Technical and Commercial proposals in the enclosed formats only. The tender will be liable for rejection if there are any deviations in format.

i. DTAP will not accept delivery of proposal in any manner other than that specified in this RFP. Proposal delivered in any other manner shall be treated as defective, invalid and rejected.

ii. Technical proposal should not contain any commercial information.

iii. A board resolution authorizing the bidder to sign/ execute the proposal as a binding document and also to execute all relevant agreements forming part of RFP shall be included in the technical proposal. Please provide complete chain of documents showing initial delegation by the board and any further sub delegation.

iv. The proposals shall be valid for a period of Twelve (12) months from the last date of submission of the bid/proposals. A proposal valid for a shorter period shall be rejected as non-responsive.

2.9.1 Proposal Preparation Costs

i. The Bidder shall be responsible for all costs incurred in connection with participation in the RFP process, including, but not limited to, costs incurred in conduct of informative and other diligence activities, participation in meetings/discussions/presentations, preparation of proposal, in providing any additional information required by DTAP to facilitate the evaluation process, and in negotiating a definitive contract or all such activities related to the bid process.

ii. DTAP will in no event be responsible or liable for those costs, regardless of the conduct or outcome of the bidding process.

2.9.2 Language of Proposal

The proposal and all correspondence and documents shall be written in English. The bidder shall furnish certified translated documents, wherever the citations/documents attached as part of the bid are in language other than English

2.9.3 Authenticity of the information and right of verification

a. DTAP reserves the right to verify all statements, information and documents submitted by the bidder in response to this RFP for the purpose of Pre-Qualification, Technical Qualification and Commercial proposal. Any such verification or lack of such verification by DTAP shall not relieve the respondent of its obligations or liabilities hereunder nor will it affect any rights of DTAP there under.

b. In case it is found during the evaluation of the responses or at any time during the subsequent procurement or project execution process, that the bidder has made material misrepresentation or has given any materially incorrect or false information in the proposal:

i. The bidder shall be disqualified forthwith (if not yet awarded the agreement either by issue of the letter of intent or entering into an agreement).

ii. DTAP would initiate appropriate action against the selected bidder as per the laws of the land, if the agreement is already awarded.

2.9.4 Venue and Deadline for Submission of Proposal

The response to RFPs must be submitted on the e-Procurement portal (https://eproc.cgstate.gov.in/) by the date and time specified in fact sheet for the RFP. Any proposal submitted on the portal after the above deadline will not be accepted and hence shall be automatically rejected. DTAP shall not be responsible for any delay in the submission of the documents.

2.9.5 Rights to the Content of the Bid Proposal

All proposals and accompanying documentation of the proposal will become the property of DTAP and will not be returned after opening of the bid. DTAP is not restricted in its rights to use or disclose any or all of the information contained in the proposal to experts/ consultants engaged in the evaluation of bid responses and can do so without compensation to the bidders. DTAP shall not be bound by any language used by the bidder in the proposal indicating the confidentiality of the proposal or any other restriction on its use or disclosure.

2.9.6 Acknowledgement of Understanding of Terms

By submitting a proposal, the bidder shall be deemed to acknowledge that the bidder has carefully read all sections of this RFP, including all forms, schedules, Annexures and Appendices hereto, and has fully informed itself as to all the conditions and limitations.

2.9.7 Format of submission

The bidders should submit their responses as per the format given in this RFP in the following manner:

a) The Response to Pre-Qualification criterion, Technical Proposal and Commercial Proposal should be covered in separate envelopes super-scribing “EMD, Tender fee & Pre-Qualification Proposal”, "Technical Proposal" and “Commercial Proposal” respectively.

Cover	Category	Cover Name	Contents	Annexure
Cover 1A	To be submitted as Original Hard Copies	“EMD, Tender fee and Power of Attorney for <RFP name and reference No.>”	a. EMD (deposited by Demand Draft/ Challan in the name of “Director, Treasury Accounts and Pension, Chhattisgarh” payable at Raipur) and Cover Letter for EMD b. Tender Fee (deposited by Demand Draft/Challan in the name of “Director, Treasury Accounts and Pension, Chhattisgarh” payable at Raipur) c. Original Power of Attorney: ‘Power of Attorney to Authorized Signatory	Annexure 1 – PQ1& PQ2
	To be submitted as scanned copies Online	EMD, Tender Fee and Power of Attorney	a. EMD (deposited by Demand Draft in the name of “Director Treasury Accounts and Pension” payable at Raipur OR Challan) and Cover Letter for EMD b. Tender Fee (Demand Draft) c. Scanned copy of Power of Attorney: ‘Power of Attorney to Authorize Signatory’	Annexure 1 – PQ1 & PQ2

Cover	Category	Cover Name	Contents	Annexure
Cover 1B	Pre-Qualification Proposal (Online Submission Only)	Pre-Qualification Proposal	a. Pre-Qualification Bid Covering Letter b. Compliance List of Pre-Qualification c. Details of Bidder Organization d. Audited financial statements (Balance Sheet, P&L statement and Cash Flow statement) in last three (3) financial years for which audited financial statements are available e. Certificate from the Statutory Auditor/CA on Bidder's Annual Turnover f. Stamped Certificate from the Statutory Auditor/CA on turnover details from MSP in Cloud and Data Centre Infrastructure services Work for the last three (3) financial years for which audited financial statements are available. g. Certificate from the Statutory Auditor/CA on net worth in the last three (3) financial years for which audited financial statements are available. h. Non-Blacklisting self-declaration by the Bidder on its letterhead as per Annexure 1 form –PQ8. i. Self-Declaration by bidder on its letterhead that company has not been declared insolvent/ bankrupt or should not have filed for insolvency/ bankruptcy or in the process of being declared bankrupt before any designated authority. j. Valid certificate for CSP from MeitY for empanelment k. Copy of valid certifications in the name of the CSP as mentioned in CSP Qualification (valid on the date of bid submission) l. Third Party Audited/Applicable reports to be submitted for valid accreditations m. Public URL and CSP Self Confirmation on CSP letterhead from authorized signatory n. Document showing the technical	Annexure 1 - a. PQ3 b. PQ4 c. PQ5 d. PQ6 e. PQ7 f. PQ8 g. PQ9 h. PQ10 i. PQ11

Cover	Category	Cover Name	Contents	Annexure
			capability of the bidder*. o. No Deviation Certificate p. Total Responsibility Declaration q. No Conflict-of-Interest Declaration r. Signed RFP and all corrigendum Note*: - *I. Work Order/ Contract clearly highlighting the scope of work and value of the contract/ order* *II. Satisfactory Performance Certificate as well as Completion/ Ongoing Certificate issued and signed by the competent authority of the client entity on it's letterhead.* *Please also refer to compliance sheet (Form-PQ4: Compliance to Pre-Qualification Criteria) and formats mentioned in Annexure-I.*	
Cover 2	Technical Proposal (Online Submission Only)	Technical Proposal	a. Technical Bid Covering Letter b. Compliance Sheet for Technical Proposal c. Unpriced Bill of Material (BOM) for the solution d. Manufacturer's Authorization Form (all applicable OEMs) and CSP Authorization Form e. Documents in accordance with CSP Criteria Compliance *Note: Please also refer to compliance sheet* (Form:TQ-2) *and formats mentioned in Annexure-II.*	Annexure II - a. TQ1 b. TQ2 c. TQ3 d. TQ4
Cover 3	Commercial Proposal (Online Submission Only)	Commercial Proposal	a. Commercial Bid Covering Letter b. Commercial Proposal Forms	Annexure III - CP1& CP2

b) Please note that prices should not be indicated in the Pre-Qualification Proposal or Technical Proposal but should only be indicated in the Commercial Proposal. In case the Prices are found in either Pre-Qualification Proposal or Technical Proposal, the Bid will be summarily rejected.

c) All the pages of the proposal must be sequentially numbered and must contain the list of contents with page numbers. Any deficiency in the documentation may result in the rejection of the Bid.

d) The Bid shall not contain interlineations or overwriting, except as necessary to correct errors made by the bidder itself. Any such corrections must be initialed by the person (or persons) who sign(s) the proposals.
e) The bid submitted shall be by the authorized signatory of the Bidder in whose name the Power of Attorney has been assigned for this RFP. In case any clarifications are sought during bid evaluation process, all the pages of response document shall be initialed and stamped by the authorized signatory.
f) The bid shall be as per the formats given in the RFP document only, no other format will be acceptable.
g) DTAP will not accept delivery of the bids by fax / e-mail or any other electronic / non-electronic means other than as specified herein.

2.9.8 Non-Responsive Proposals

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

a) If it does not comply with the terms & conditions, requirements of this RFP, failure to comply with the technical requirements, and acknowledgment of receipt of amendments
b) If a proposal appears to be "canned" presentations of promotional materials that do not follow the format requested in this RFP for Technical and Commercial proposals or do not appear to address the requirements of the proposed solution, and any such bids may also be disqualified.
c) If the technical or commercial proposal of the bidder does not adhere to the requirements of this RFP, the bid shall be declared as non-responsive and will not be evaluated further.

2.9.9 Authentication of Bids

A Proposal should be accompanied by power-of-attorney in the name of the signatory of the Proposal.

2.9.10 Right to the content of bid proposal

All bids and accompanying documentation of the technical proposal will become the property of DTAP and will not be returned after opening of the bid proposals. DTAP is not restricted in its rights to use or disclose any or all of the information contained in the proposal and can do so without compensation to the bidders. DTAP shall not be bound by any language in the proposal indicating the confidentiality of the proposal or any other restriction on its use or disclosure.

2.9.11 Disqualification

The proposal submitted by the bidder is liable to be disqualified if one or more of the following conditions are violated.

a) Violation of the bid submission process
    i. Commercial proposal and technical proposal are not submitted in the prescribed formats and mode as given in the RFP.
    ii. The price information, the pricing policy or pricing mechanisms or any document/information/file indicative of the commercial aspects of the proposal are either fully or partially enclosed or are part of the Technical Proposal.
    iii. If it comes to DTAP's knowledge expressly or implied, that some bidders may have compounded in any manner whatsoever or otherwise joined to form a cartel resulting in delay / holding up the processing of Bid then the bidders so involved are liable to be disqualified for this agreement.
    iv. If a bidder submits more than one bid.
b) In a tender, either the Indian agent on behalf of the Principal / OEM or Principal/OEM itself can bid but both cannot bid simultaneously for the same item/product in the same tender
c) If an agent submits bid on behalf of the principal / OEM, the same agent shall not submit a bid on behalf of another Principal/ OEM in the same tender for the same item/ product
d) Non-compliance to the conditions of the bidding process
    i. The Bid documents are not signed as per guidelines of the RFP

ii. The required EMD has not been submitted as specified in the RFP
iii. The Bid validity period is shorter than the required period
iv. The Bid is not submitted in accordance with this document
v. During validity of the Bid, or its extended period, if any, the bidder revises its quoted prices
vi. The bidder qualifies their bid with their own conditions or assumptions
vii. Bid is received in incomplete form
viii. Bid is not accompanied by all the requisite documents

e) Nonresponsive Content of the proposal
   i. Information submitted in technical proposal is found to be misrepresented, incorrect or false, accidentally, unwittingly, or otherwise, at any time during the processing of the bids or during the tenure of the agreement including the extension period, if any
   ii. The deliverables as given in the technical proposal should be in consonance with the Commercial proposal. Any deviations in the final deliverables between Technical and Commercial proposals shall make the Bid as being unresponsive and may lead to disqualification of the Bid

f) Inability to respond in accordance with the bidding guidelines
   i. The successful bidder, invited to sign the agreement qualifies the letter of acceptance of the agreement with its own conditions
   ii. The successful bidder fails to deposit the Performance Bank Guarantee or fails to enter into an agreement within such period specified by DTAP.

g) Fraudulent and corrupt practice
   i. Bidder tries to influence the proposal evaluation process by unfair/unlawful/corrupt/fraudulent means at any point of time during the bid process defines, for the purposes of this provision, the terms set forth below as follows:
   ii. "Corrupt" practice means the offering, giving, receiving, or soliciting of anything of value to influence the action of a public official in the procurement process or in agreement execution; and
   iii. "Fraudulent" practice means a misrepresentation of facts in order to influence a procurement process or the execution of an agreement to the detriment of the Purchaser, and includes collusive practices among bidders (prior to or after bid submission) designed to establish bid prices at artificial, non-competitive levels and to deprive the purchaser of the benefits of free and open competition;

h) Consequences of disqualification
   i. If a bid or a proposal is disqualified, the bidder will not be eligible to participate in the bidding process initiated by this RFP.
   ii. If the proposal/bid is disqualified, it will not be processed further and the same will be communicated to the bidder. No further correspondence from the bidder with DTAP will be entertained.
   iii. If the disqualification is for the reasons of fraudulent or corrupt practice, DTAP has the right to initiate actions to blacklist the bidder as per the provisions of the relevant acts/rules.

2.9.12 Commercial Bid Format

a) The Bidder must submit the Commercial Bid in the formats specified in Annexure III of this RFP. The Bidders shall give the required details of all applicable taxes, duties, other levies and charges etc. in respect of provision of services under this RFP.
b) The bidders shall quote an all-inclusive bid value in their commercial bids.
c) The Bidders shall quote for the entire scope of contract on an "overall responsibility" basis such that the quote for the project covers all obligations of the bidder mentioned in the Bidding documents in respect of providing the services.
d) The bidder shall submit a priced bill of quantities as part of the commercial bid. The format of the priced bill of quantities as specified under Annexure III of this RFP should be used.

e) Bidders are advised to exercise adequate care in quoting the prices. No excuse for corrections in the quoted price will be entertained after the bids are submitted. All corrections, if any, should be initialed by the person signing the bid form before submission.

f) Notwithstanding any price (s) quoted in the offer across different sections of the bid, only prices given in the prescribed format given at Annexure III of this RFP shall prevail.

g) Price quoted by the Bidder shall remain firm during the entire contract period and shall not be subject to variation on any account except change in applicable tax rates (e.g. GST) or change in scope.

h) A bid submitted with an adjustable price quotation or conditional bid may lead to disqualification of the bidder. DTAP reserve the right to take appropriate action in this regard.

i) If a bidder costs NIL charges as ‘Total Contract Value’, the bid shall be treated as unresponsive and will not be considered for further evaluation.

2.10 Bid Opening and Proposal Evaluation

2.10.1 Bid opening sessions

a. The Proposals submitted up to last date and time (refer Fact Sheet) will be opened at specified date and time (refer Fact Sheet) by the Nodal Officer or any other officer authorized by the DTAP, in the presence of the Bidder’s representatives who may be present at the time of opening.

b. The representatives of the Bidders are advised to carry an identity card or a letter of authority from the Bidding entity to identify their bonafides for attending the opening of the Proposal.

2.10.2 Proposal Validity

a. The proposal submitted by the Bidders should be valid for Bid Validity Period (refer fact sheet) from the date of submission of the Proposal.

b. DTAP may request the Bidder(s) for an extension in period of validity of the bid. The validity of the EMDs should also be suitably extended if called upon to do so by DTAP.

2.10.3 Pre-Qualification Evaluation

Following are the pre-qualification requirements for the bidders: -

S. No.	Eligibility Criteria	Criteria Description	Documentary proof to be submitted
Basic Bid Related Fees/Documents			
1	**Tender Fee**	Tender Fees of the amount mentioned in Bid Control Sheet. The Tender Fees should be as per the provisions of Bid Fact Sheet.	Copy of DD/ Challan as deposited for Tender document fee in the name of "Director Treasury Accounts and Pension, Chhattisgarh" payable at Raipur.
2	**EMD**	The bidder should furnish, as part of its proposal, an Earnest Money Deposit (EMD) of amount mentioned in Bid Control Sheet. The EMD should be as per the provisions of Bid Fact Sheet.	a. Scanned copy of DD or Challan (to be submitted along with bid) b. Demand Draft or Challan (to be submitted physically to communication address mentioned in Bid Control Sheet on or before the last date and time of bid submission)
3	**Power of Attorney (PoA)**	The Board resolution and Power of Attorney in the name of the person signing the bid.	Board Resolution, 'Power of Attorney to Authorize Signatory' (Format Specified in Annexure-I) a. Scanned copies of document to be submitted online on e-Procurement Portal b. Original document (to be submitted physically to communication address mentioned in Bid Control Sheet on or before the last date and time
Legal Entity, Blacklisting Criteria and Financial Strength – MSP Qualification			
4	**Legal Entity**	The Bidder/MSP shall be legal entity and registered in India with following criteria: I. Should be Company registered under Companies Act, 2013 or 1956, amended till date or a Limited Liability Partner incorporated under Limited Liability Partnerships Act, 2008 II. Should be in existence for at least ten years as on 31/03/2024. III. Registered with GST Authority in India	a. Certificate of Incorporation of the Company/LLP b. Copy of PAN & TAN c. Copy of Registration Certificates with the GST Authority d. Copy of Income Tax and GST returns for last 2 financial year (FY 2022-23 and FY 2021-22) (To be submitted in the format provided under Form – PQ 5)
5	**Declaration for not being blacklisted *(as on Date of***	The Bidder/MSP should not have been blacklisted (as on date of submission of bid) by any entity of Govt. of India, any State	Self-Declaration by bidder on its letterhead as per Annexure I Form *(To be submitted in the format provided*

S. No.	Eligibility Criteria	Criteria Description	Documentary proof to be submitted
	submission of bid)	Government in India, Government Agencies, Public Sector Undertakings, or any Autonomous organization of Central or State Government for participation in future bids for unsatisfactory past performance/ corrupt/ fraudulent, or any other unethical business practices	*under Form – PQ 8)*
6	**Insolvency / Bankruptcy**	The Bidder/MSP must not have been declared insolvent/ bankrupt or should not have filed for insolvency/ bankruptcy or in the process of being declared bankrupt before any designated authority.	Self-Declaration by bidder on its letterhead that company has not been declared insolvent/ bankrupt or should not have filed for insolvency/ bankruptcy or in the process of being declared bankrupt before any designated authority.
7	**Average Annual turnover of MSP from Cloud Services or Data Center Establishment Services or IT Services**	The Bidder/MSP should have an average annual turnover from Cloud Services or Data Center Establishment Services or IT Services of Rs. 10 Crores or more in the last three (3) financial years for which audited Financial Statements are available sk	Stamped Certificate from the Statutory Auditor/CA on turnover details of CSP from Cloud services or Data Center Establishment Services Work for the last three (3) financial years for which audited financial statements are available. *(To be submitted in the format provided under Form – PQ 6)*
8	**Annual Turnover**	The Bidder/MSP should have annual turnover of INR 25 Crores each in last 3 financial years .	CA Certificate and certified copy of turnover to be submitted
9	**Positive Net worth**	**<u>Positive Net Worth in each of the last 3 Financial Years:</u>** Bidder/MSP should have positive net worth for latest three (3) financial years for which audited financial statements are available	Certificate from the Statutory Auditor/CA on net worth in the last three (3) financial years for which audited financial statements are available. *(To be submitted in the format provided under Form – PQ 6)*
10	**Experience with Government/PSU**	Bidder/MSP should have experience working with Government client/PSU with similar nature of financial project for supply of database licenses/ migration of database with minimum order value of 2 Crores.	Work Order/ Completion certificate
CSP Qualification			

S. No.	Eligibility Criteria	Criteria Description	Documentary proof to be submitted
11	**MeitY empanelment**	The cloud services offered by the Bidder should provide Meity empanelment certificate for the Cloud Service Provider (CSP).	Valid certificate from MeitY.
12	**MAF from CSP and Oracle Database Licenses**	Bidder/MSP should provide undertaking from CSP regarding authorization for providing cloud and oracle database Licenses.	Undertaking from CSP. MAF from CSP and MAF for Oracle database Licenses.
13	**Certifications**	The CSP should have the following Cloud Security Certificates of proposed cloud service I. **ISO27017-** cloud service security II. **ISO27018-** protection of personal data in the cloud III. **ISO27701-**privacy information management system IV. **Tier-3 certification**– A data center with multiple paths for power and cooling, and redundant systems that allow the staff to work on the setup without taking it offline.	Copy of valid certifications in the name of the CSP (valid on the date of bid submission)
14	**Accreditations**	The CSP should provide the cloud service having accreditation relevant to security, availability, confidentiality, processing, integrity and privacy trust services principles SOC1, SOC2/SOC3 (System and Organization Control), PCIDSS	Third Party Audited/Applicable reports to be submitted.
15	**Unit Price Listing**	The “Listed unit price” (Price List) of all the services offered by CSP should be publicly available on the CSP portal. The Bidders shall also submit the “Listed unit price” for all the BOQ components along with the technical bid.	Public URL and CSP Self Confirmation on CSP letterhead from authorized signatory
16	**Technical Capability-Experience in Cloud Infrastructure Services**	Bidder/CSP should have Completed at least one project of cloud infrastructure services with similar nature involving hosting of financial application and database in cloud environment to any Government Organization /PSU/Banking Application with minimum value of 2 Crores.	Work Order/ Contract/Self Declaration clearly highlighting the scope of work and value of the contract/ order

S. No.	Eligibility Criteria	Criteria Description	Documentary proof to be submitted
17	**Relevant resources onboard**	The CSP/MSP must have on its roll at least 5 technically Cloud Certified professionals and prior experience in providing the Cloud/ Data Centre Infrastructure services on the date of submission of the bid.	Certificate by Human Resources Department of the CSP on CSP's letter head.

a. DTAP shall open and validate the contents of Cover 1
b. If the response to "pre-qualification" is received as per requirements and prescribed format, then DTAP shall evaluate the response to the Pre-Qualification requirements in accordance with the Pre-qualification requirements specified in this RFP.
c. The Pre-Qualification bid must contain all the documents mentioned in "Annexure I - Pre-Qualification Bid Templates". Each of the Pre-Qualification condition mentioned in this section is mandatory. In case the Bidder does not meet any one of the conditions, the bidder will be disqualified.
d. Technical and Commercial bids for those bidders who do not pass the pre-qualification stage, will not be opened.
e. A checklist must be created by the bidder and be submitted along with the proposal with proper page-wise indexing of all supporting documents.

2.10.4 Technical Qualification Evaluation

a. The technical evaluation will be performed for only those bidders whose proposal qualifies in the pre-qualification evaluation.
b. The relevant technical compliance sheet is provisioned in Annexure II Form- TQ2 of this RFP. The bidder is required to fill the technical compliance sheet mandatorily and submit along with the technical proposal. Also, the bidder is required to comply minimum 90% of the line items mentioned under all respective category of the requirements.
c. In case a bidder does not comply with any line item in the respective category of technical compliance, in such a situation, at any later time if the project is required to deliver the line item by the CSP for smooth functioning. Applications are required to be procured by the MSP through any means necessary to meet the project requirements.

***Note**: DTAP reserves the right to check/ validate the authenticity of the information provided in the Pre-qualification and Technical Evaluation criteria and the requisite support must be provided by the Bidder.*

2.10.5 Commercial Evaluation

All the technically qualified bidders or their authorized representative may present at the time of opening the Commercial Bid, it can be seen automatically in e-procurement site.

a. The Commercial Proposal (Cover 3) for the technically qualified bidders shall be opened online and reviewed to determine whether the commercial bids are substantially responsive. Bids that are not substantially responsive are liable to be disqualified at BEC's discretion.
b. The bid price shall be in Indian Rupees (INR). Any applicable taxes and levies are to be included in the bid price.
c. For the purpose of commercial evaluation, Total Bid Value (TBV) as captured by bidder in the Commercial Bid 'Form 14.2.1 Summary of Costs' shall be considered.
d. Only fixed price commercial bids indicating total price for all the deliverables and services specified in this bid document will be considered.
e. Commercial Bids that are not as per the format provided under the heading titled 'Formats for Commercial Bids' shall be liable for rejection.

f. If there is a discrepancy between words and figures, the amount in words will prevail.
g. Arithmetical errors will be rectified on the following basis: "If there is a discrepancy between the unit price and the total price that is obtained by multiplying the unit price and quantity, the unit price shall prevail, and the total price shall be corrected.
h. Any bids submitted with conditions shall be rejected;
i. The evaluation will be on the unit price exclusive of taxes. Taxes and other liabilities as per the applicable rates and to be paid as per actuals.
j. The offers shall be evaluated and marked L1, L2, L3 etc. L1 being the lowest offer
k. It shall be ensured that the offer recommended for sanction is justifiable looking to the prevailing market rates of the goods, works or service required to be procured.
l. The tender shall be awarded on L1 selection basis from amongst the net commercial bids value of bidders. In case of two L1 then selection will be done on negotiation basis.
m. Further, negotiations will be conducted with the successful (L1) bidder for improvement in the scope of work, specification, further reduction in bid price & in price discovery rates and advancement of delivery schedule.
n. In Case, (L1) successful bidder fails to provide the service due to any circumstances arises during the project period, L2 or L3 bidder will be approached to provide service on the quoted L1 rate.

2.11 Appointment of Successful Bidder

2.11.1 Signing of Agreement

a. Upon notification of the outcome of the commercial evaluation, DTAP shall issue a Letter of Intent before entering into an agreement with the successful bidder. The draft agreement is provided in RFP.
b. The successful bidder shall submit a fresh undertaking of not being blacklisted as on date of the signing of the agreement.
c. Notwithstanding any delay in signing of agreement, upon acceptance of letter of intent the bidder shall commence work on the project.
d. DTAP shall have the right to annul the award in case there is a delay of more than 30 days in signing of agreement, for reasons attributable to the successful bidder.
e. DTAP does not commit to buy all the items in the quoted price for which pricing has been sought. Out of the various priced items of the Commercial proposal, DTAP will have the option and the right to buy any combination of services or items. The priced items which DTAP intends to buy will be included in the commercial agreement with the successful bidder.
f. During the period of the agreement, DTAP could buy any of those items which are not included in the agreement, and which are part of the quoted price of the bidder. DTAP will have the right to buy those services at the same rate for which the bidder was selected as the successful bidder. The Price quote for all the services indicated in the quote will be valid for the complete period of agreement.
g. Once an agreement is signed with the successful bidder based on the commercial proposal, no adjustment of the agreement value shall be made on account of any variations in costs of labour and materials or any other cost component affecting the total cost in fulfilling the obligations under the agreement.
h. The agreement value arrived at shall be the only payment payable by DTAP to the bidder for completion of the contractual obligations by the successful bidder under the agreement, subject to the terms of payment specified in this document. The price would be exclusive and inclusive of all taxes, duties, charges and levies as applicable.

2.11.2 Acceptance of Letter of Intent (LoI)

The successful bidder shall submit in writing the acceptance of the terms and conditions of the LoI within the time prescribed by DTAP. Failure of the successful bidder to provide the acceptance within given time frame shall constitute sufficient grounds for the annulment of the award of LoI. In such event DTAP may issue LoI to the next bidder or call for new proposals.

2.11.3 Performance Bank Guarantee

a. PBG of 3% of value of the agreement (Total Contract Value) would be furnished by the bidder in the form of a Bank Guarantee as per the format provided in this RFP from Nationalized Banks or scheduled bank. The PBG should be furnished within 15 days from the signing of the agreement and should be valid till the entire term of the agreement and for an additional period of one year after the completion of term of agreement including warranty obligations. Bid security would be refunded to the successful bidder on receipt of Performance Bank Guarantee.

b. All incidental charges whatsoever such as premium; commission etc. with respect to the performance bank guarantee shall be borne by the bidder. If the project implementation/go- live is delayed, the PBG shall be extended by the bidder for such additional duration. The performance bank guarantee may be discharged/ returned by DTAP upon being satisfied that there has been due performance of the obligations of the bidder under the agreement. However, no interest shall be payable on the performance bank guarantee.

c. In the event of the bidder being unable to service the agreement for whatever reason, DTAP would invoke the PBG. Notwithstanding and without prejudice to any rights whatsoever of DTAP under the agreement in the matter, the proceeds of the PBG shall be payable to DTAP as compensation for any loss resulting from the bidder’s failure to perform/comply its obligations under the agreement. DTAP shall notify the bidder in writing of the exercise of its right to receive such compensation within 7 (Seven) days, indicating the contractual obligation(s) for which the bidder is in default.

2.11.4 Conflict of Interest

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

2.11.5 Amendment of the RFP

At any time prior to the deadline for submission of the proposals, DTAP, for any reason, may modify the RFP by amendment and it shall publish it in the same manner as mentioned in the Bid control sheet. Such amendments shall be binding on the Bidders.

2.11.6 Legal Obligations of the bidder

The Bidding Process shall be governed by and construed in accordance with the laws of India and the Court at Raipur shall have exclusive jurisdiction over all disputes arising under, pursuant to and/or in connection with the Bidding Process.

The actions stipulated in this RFP are without prejudice to any other legal action that may follow in accordance with the provisions of any other law in force relating to any civil or criminal proceedings by any competent court in India.

3. ***PROJECT TIMELINES, PAYMENT TERMS, SCHEDULES &MILESTONES***

3.1 Project Timelines

SL. NO.	Description	Timeline (Tentative)
1.	Issuance of LOI	T+1 week
2.	Provisioning of a) DC & DR b) Network Connectivity	T+5 week
3.	Migration of the application on the Cloud environment	T+9 week
4.	Operational Acceptance (OA)	T+11 week
5.	Operation and Maintenance phase	Will start from the date of OA provided by DTAP.

3.2 Payment Terms

a. The Invoice will be generated & submitted, after DTAP approval of every Milestone. If all things are verified within the norms, DTAP will endeavor to expedite the payment after submission of Invoice.

b. All payments agreed to be made by DTAP to the MSP in accordance with the Bid shall be inclusive of all, statutory levies, duties, taxes and other charges whenever levied/ applicable including costs of maintenance, if any and DTAP shall not be liable to pay any such levies/ other charges under or in relation to this Contract and/ or the Services.

c. No invoice on account of change order will be submitted by the selected bidder unless the said extra work/ change order has been authorized/approved by DTAP in writing.

d. The payment shall be made to the MSP after deduction of all applicable penalties, taxes, etc.

e. In case of any changes by Government in taxes, then actual taxes on the date of billing would prevail.

f. All costs, damages or expenses, which DTAP, may have paid or incurred, for which under the provisions of the Contract, the MSP is liable, and DTAP shall deduct the same from any dues to the MSP. All payments to the MSP shall be made after making necessary deductions as per terms of the Contract.

g. For Products and/ or Services supplied locally, the MSP shall be entirely responsible for all taxes, duties, license fees, etc., incurred until delivery of the contracted Products or Services to DTAP.

h. For the cloud hosting charges operation & Maintenance Cost, MSP shall quote an estimated monthly charge as per annexure III section 13.2.3. The payments from DTAP shall be made on actual basis as per the invoice of the Cloud Service Provider. No cost escalation will be accepted by DTAP in this regard during the duration of the contract. The bidder is expected to consider industry best practices to optimize the hosting charges thus reducing DTAP total cost of ownership.

i. The bidder is expected to account for all services/ hardware/ software/ hosting required to make the implementation successful as part of total contract value.

j. DTAP reserve the right to increase or decrease the no. of resources / other items quantity at the time of Agreement or during the project.

3.3 Payment Schedule

S. No.	Milestone No.	Deliverable / Milestone	Fee to be paid
A	**Additional License Supply**		**Cost Item in A1 - a**
1	M1	License Supply as per Schedule-I Part A	As per actual quoted in commercials (On Successful commissioning of the servers)
B	**Implementation Charges**		**% of Cost Item (A1 – b + c)**
2	M2	Successful initial setting up of the Cloud Environment (DC+DR) and acceptance by DTAP	30% (On Successful commissioning of the servers)
3	M3	Successful hosting of the applications and data migration of existing system to Cloud environment and sign-off from the Government Department / Agency	70% (On Successful Go-Live and Acceptance)
C	**Operations & Maintenance Costs - Monthly Payments** (The first monthly payment will be due on completion of one month from the date of successful Completion of Migration and sign off from the Government Department/Agency)		**Capped with cost item in (A2 – a + b)**
4	M4	Cloud Services as per Schedule – I Part B	This shall be paid on actuals on a quarterly basis based on Cloud Service Provider invoices (capped by respective month cost quoted by Bidder in Form A2 – paid quarterly).
C	**Manpower Deployment**		**Cost Item in A2 – c**
5	M5	For deployment of the resources paid post Go-Live of the project	As per actuals monthly cost quoted for the manpower deployment (paid quarterly).

Note - Payment for Managed Services:

1. EMI will be made at the end of the quarter after satisfactory delivery of the services
2. Total Quarterly payment will be linked to the compliance with the SLA metrics and the actual payment due to the MSP after any SLA related deductions.
3. Additional Services: Government Department / Agency will have the option to avail the additional services of MSP for carrying out any extension or changes in services, as part of the project.

4. ***CONTRACT PERIOD***

Tenure of Contract: The tenure of the contract shall be for a period of three years.

Extension of contract: The contract may be extended for a further period at the sole discretion of Directorate of Treasuries & Accounts, Chhattisgarh.

5. MANPOWER DEPLOYMENT

The successful bidder needs to deploy onsite- at client location, well qualified and experienced resources having in-depth knowledge and experience of the position for which they are deployed mentioned below. The resources shall have to carry out work in order to meet the desired objectives of implementing and running the IFMIS System.

The table given below provides the minimum qualification details, no. of resources required at onsite and responsibilities of the required manpower. The successful bidder is expected to adhere with the requirements and deploy relevant resources for the project.

5.1 Manpower Qualification & Responsibilities

S. No.	Position	Education and Experience Requirements	Number of profiles to be submitted	Responsibilities
C1	**Cloud Support Engineer**	**Education and Certifications** i Minimum B.Tech/B.E./ MCA ii Any leading Cloud certification iii Fluency in English and Hindi (Speaking, reading & writing) **Experience** At least 3 years of experience in supporting cloud-based solution of large IT/ITeS projects in the role of cloud support engineer (projects in Government Sector/Public Sector/Private Sector)	1	• Monitoring the hardware deployed in Cloud infrastructure • Manages and supports the Dev to Production cloud platform, to ensure quality, performance and availability of hosted services • Deploying application, patches in multiple environments

5.2 Replacement of Personnel

I. The Bidder should to the best of its efforts, avoid any change in the organization structure and proposed manpower proposed for execution of the scope of services or replacement of any manpower resource.

II. If the same is however unavoidable, due to circumstances such as the resource leaving the MSP's organization, MSP shall promptly inform the DTAP in writing, and the same shall require subsequent approval by the DTAP. SI should ensure that they adhere to the SLA for replacement of manpower as defined in this RFP.

III. In case of replacement of any manpower resource, the MSP should ensure efficient knowledge transfer from the outgoing resource to the incoming resource and adequate hand-holding period and training for the incoming resource in order to maintain the continued level of service.

5.3 Removal of Personnel

I. DTAP may at any time object to and request the MSP to remove from the sites any of MSP's authorized representatives including any employee of the MSP deployed at site for professional incompetence or negligence or for being deployed for work for which he is not suited.

II. DTAP representative shall state to the MSP in writing its reasons for any request or requirement pursuant to this clause. The MSP shall promptly replace any person removed, pursuant to this section, with a competent substitute, and at no extra cost to the DTAP.

5.4 Logistics requirements of the Personnel

The MSP shall be responsible for the deployment, transportation, accommodation and other requirements of resources deployed for the execution of the work and provision of services for all costs/charges in connection thereof.

6. *DEPLOYMENT AND ARCHITECTURE*

a) Application is Windows .net based framework, operating system will be Windows Server.

b) The Application will reside on infrastructure services – the license for Windows should be as a managed service from CSP.

c) Database services must be CSP native managed database platform services for DC & DR. The DR should preferably run-on minimum compute to replicate the changes of the DC. In case of DR Failover or switch over DR must scale to full and equivalent compute as of DC. In this case bidder should follow database OEM licensing policy to remain compliant to get database OEM support.

d) The database should be on Oracle 19C enterprise edition with options or above version. Bidder should consider below for database provisioning.

- Provision of at-least 10 TB of usable SSD block storage.
- Provision of at-least 10 TB of usable object storage.
- Should keep at-least one full database backup on object storage (on weekly basis).
- Should have provision for automated backup and database recovery.

e) Bidder should offer CSP native database backup tool to back up the databases. Database Backup Cloud Service should automatically and transparently replicate the data across multiple storage nodes in the same geographic region, which provides instant availability.

f) Database Backup Cloud Service should protect data by providing end-to end security.

g) The bidder should provision of a fully managed data protection service for Oracle databases. This service must exhibit automated features ensuring real-time protection of Oracle Database alterations, validating backups without imposing overhead on production databases, and facilitating rapid, predictable recovery to any designated point in time to access the resilience of zero data loss.

h) Bidder should offer database protection to recover protected databases to within less than a second of when an outage or ransom ware attack occurred.

i) Bidder should offer automatic database protection and lifecycle management minimize administration time, improve the efficiency of production database services, and help consistently secure critical information.

j) Bidder should also provide Oracle database Data Safe service as a CSP native managed service to understand data sensitivity, evaluate data risks, mask sensitive data, implement and monitor security controls, assess user security, monitor user activity, and manage Oracle Database—all in a single, unified console to manage the day-to-day security and compliance requirements of Oracle Databases.

k) Bidder should offer 99.9% SLA on Oracle database system. This should be separate from infrastructure SLA defined in the RFP.

l) Bidder to consider Transparent Data Encryption (TDE) to transparently encrypt data at rest in Oracle Databases. It should stop unauthorized attempts from the operating system to access database data stored in files, without impacting how applications access the data using SQL. It should encrypt entire application table spaces or specific sensitive columns. It should fully integrate with Oracle database.

7. SCOPE OF WORK

Directorate of Treasuries, Accounts & Pension, Government of Chhattisgarh wishes to engage a Managed Service Provider through MeitY empaneled Cloud Service Provider for providing Cloud Services for hosting the IFMIS applications for a period of 3 years, with the possibility of an extension upon completion of the third year, at the discretion of the DTAP.

The selected bidder will be responsible to fulfill below mentioned scope of work which includes, but is not limited to, the following:

1 **Setup the cloud account with the proposed Cloud service provider:** The bidder will be responsible for lifting up the existing e-Kosh Application and shifting the application in virtual public cloud environment without making any changes in the existing application. The Bidder will provide cloud services for setting up, installation, configuration, management, upgradation, migration of application servers, database servers/storage, security etc. and also maintain and manage and configure the VMs, Containers, Storage, Network, Database etc.

2 **Provide cloud services:** The selected bidder shall provide Infrastructure as a Service (IaaS) from MeitY empanelled Cloud Service Provider (CSP) which includes fundamental resources such as compute, storage, networks and others, where the consumer can deploy and run any software they choose. The bidder will manage and control the underlying Cloud infrastructure including operating systems, storage, network, security, etc. The User Department will have control over the deployed applications and possible configuration settings for the application-hosting environment. The bidder will also provide Platform as a Service (PaaS) which includes the Cloud infrastructure and platform (such as middleware) to run the applications created using programming languages, libraries, services, and tools supported by the CSP. Users will be able to securely load applications and data onto the computing or virtual machine instance from the SSL VPN clients only and not from the public internet. The bidder will be responsible for providing adequate compute, storage and network services for hosting the IFMIS application and database in the cloud. The proposed deployment plan for the IFMIS application includes:

- Production
- Development/Testing
- Staging
- Disaster Recovery

3 **Support NIC Data Center:** The Bidder will support e-Kosh NIC Data Center, Mahanadi Bhawan (Naya Raipur, Chhattisgarh) for implementation, management, and monitoring of IFMIS software in cloud environment. DDOS, IPS, IDS Services, anti-malware, vulnerability scanning and penetration testing etc to be configured for IFMIS application and ensure 99.9 % uptime of cloud services as per agreement. Bidder will also be responsible for providing 24x7x365 support to NIC Data Center in case of any issues related to the cloud services and connectivity.

4 **Migration of applications and databases:** The Bidder will be responsible for migrating to cloud in co-ordination with the NIC Data Center and should ensure to meet all standard data formats for data transfer /portability during migration. The Bidder is expected to understand the complete architecture of existing applications and processes necessary for smooth migration of applications and databases including interdependencies between applications and data. The Bidder shall be responsible for deployment of security patches on cloud platform in co-ordination with the NIC Data Center. It should also be noted by the bidder that:

1. Database should have native, active-active clustering with objectives of scalability and availability of 24x7. It is capable of masking outages from end users and applications by recovering the in-flight database sessions following recoverable outages. All the nodes of cluster should be able to perform Read & Write Operations on a single database simultaneously from all the nodes.
2. One Application will be deployed on internet while other Application would serve only to Specific Treasuries via intranet.
3. Strength with all Integrations. Database in DR should be in Oracle Active Data Guard Configuration and Open with Read Only Mode So that real time reporting can be done from DR.
4. App Server and Integration Server in DC and DR should be in Sync.
5. Note: VM Configurations should be such that resources can be scaled up or scaled down, based on the requirements and specific time of the day.
6. RPO Should be 30 minutes and RTO Should be 1 hour.

5 **Data Management**

a. Bidder should always ensure that data is destroyed whenever any cloud virtual machine is recycled or deleted. The data destruction policy of CSP should be shared with the Purchaser within 15days after LoI.
b. Bidder should clearly define policies to handle data in transit and at rest.
c. Bidder should not delete any data at the end of contract period without consent from the Purchaser.
d. In case of scalability like horizontal scalability, the Bidder should ensure that additional generated data is modify/deleted with proper consent from the Purchaser.
e. Bidder should ensure secure data transfer between DC and DR site.
f. Bidder shall put in place a system to prevent data leakage protection and prevention.

6 **Storage**

a. Bidder should provide scalable, dynamic and redundant storage.
b. Bidder should offer to auto allocate more storage as and when required based on storage utilization threshold and also offer to provision from self-provisioning portal to add more storage as and when required by the Purchaser.
c. Bidder should clearly differentiate its storage offering based on IOPS. There should be standard IOPS offering per GB and high-performance disk offering for OLTP kind of workload. Bidder should be able to give multiple option for IOPS.
d. Bidder should have block disk offering as well as file/object disk offering to address different kind of the Purchaser requirements.

7 **Network**

a. Bidder must ensure that cloud virtual machine of the Purchaser is into separate network tenant and virtual LAN.
b. Bidder must ensure that cloud virtual machines are having private IP network assigned to cloud VM.
c. Bidder must ensure that all the cloud VMs are in same network segment (VLAN) even if they are spread across multi-DC of CSP.
d. Bidder should ensure that clouds VMs are having Internet and virtual network interface cards.
e. Bidder should ensure that Internet vNIC card is having minimum 1 Gbps network connectivity and service vNIC card is on minimum 10 Gbps for better internal communication.
f. In case of scalability like horizontal scalability, the Service provider should ensure that additional requirement of network is provisioned automatically of same network segment.

g. Bidder must ensure that public IP address of cloud VMs remains same even if cloud VM gets migrated to another DC due to any incident.
h. Bidder must ensure that public IP address of cloud VMs remains same even if cloud VM network is being served from multiple CSP DC.
i. Bidder must ensure that the public network provisioned for cloud VMs is redundant at every point.
j. Bidder must ensure that clouds VMs are accessible from the Purchaser private network.
k. Bidder must ensure that there is console access to cloud VMs, if the Purchaser requires accessing it.
l. Bidder shall ensure that cloud VM network is IPV6 enabled and all public facing devices are able to receive and transmit IPV6 data in addition to IPV4.
m. Bidder should have provision of dedicated virtual links for data replication between their multiple DC in order to provide secure data replication for DR services.
n. Bidder should ensure use of appropriate load balancers for network request distribution across multiple cloud VMs.
o. The bid must include the necessary hardware such as routers, switches, connectors, and cable. The bidder will also be responsible for the installation, commissioning, and implementation of additional hardware at the Data Centre for the commissioning of the leased line.

8 **Compatibility**

a. Bidder must ensure that the virtual machine format is compatible with other cloud provider.
b. Bidder should be able to export the virtual machine from other Service provider cloud and use that anywhere i.e., in different CSP.
c. Bidder should provision to import cloud VM template from other cloud providers.
d. Bidder should ensure connectivity to and from cloud resources of the Purchaser is allowed to/from other cloud service providers if required and approved by the Purchaser.

9 **Root Access:** The bidder will be responsible to provide the access of root account of virtual machines of proposed CSP to NIC e-Kosh Data Center, Mahanadi Bhawan (Nawa Raipur, Chhattisgarh).

10 **Disaster Recovery Setup:** The Bidder shall offer DR as a service for all resources offered on primary DC site. Bidder shall be responsible for setting up of disaster recovery site in different seismic zone in India only as per specifications provided below:

a. The bidder would be responsible for Disaster Recovery Services so as to ensure business continuity of operations in the event of failure of primary DC and meet the RPO and RTO requirements.
b. RPO should be equal to 30 minutes and RTO shall be less than or equal to 1 hours.
c. During the change from Primary DC to DR or vice-versa (regular planned changes), there should not be any data loss.
d. There shall be asynchronous replication of data between Primary DC and DR and the Bidder will be responsible for sizing and providing the DC-DR replication link so as to meet the RTO and the RPO requirements.
e. During normal operations, the Primary DC will serve the requests. The Disaster Recovery Site will not be performing any work but will remain on standby. During this period, the compute environment for the application in DR shall be available but with minimum possible compute resources required for a functional DR as per the solution offered. The application environment shall be installed and ready for use. DR Database Storage shall be replicated on an ongoing basis and shall be available in full (100% of the PDC) as per designed RTO/ RPO and replication strategy. The storage should be 100% of the capacity of the Primary Data Centre site. This requirement could be carried out manually subject to meeting RPO/ RTO requirements.

f. In the event of a site failover or switchover, DR site will take over the active role, and all requests should be routed through DR site. The pre-requisite to route request to DR should be articulated properly and shared by service provider.

g. Whenever there is failover from primary DC to secondary (DR), compute environment for the application at DR site shall be equivalent to DC including all the security features and components of DC, without the failover components. Development/test/quality environment will not be required at DR site.

h. The installed application instance and the database shall be usable and the same SLAs as DC shall be provided.

i. The bandwidth at the DR shall be scaled up to the level of Data Centre when DR is activated.

j. The Bidder shall conduct live DR drill for two days at the interval of every six months of operation wherein the Primary DC has to be deactivated and complete operations shall be carried out from the DR Site. However, during the change from DC to DR or vice-versa (regular planned changes), there should not be any data loss. The pre-requisite of DR drill should be carried out by Bidder and NIC jointly. Certificate for DR drill should be submitted to DTAP for compliance.

k. The Bidder shall clearly define the procedure for announcing DR based on the proposed DR solution. The Bidder shall also clearly specify the situations in which disaster shall be announced along with the implications of disaster and the time frame required for migrating to DR. The Bidder shall plan all the activities to be carried out during the Disaster Drill and issue a notice to the DTAP and NIC at least two weeks before such drill.

l. The disaster recovery plan needs to be provided by the service provider which needs to be updated half-yearly.

m. The service provider should offer dashboard to monitor RPO and RTO.

n. Any lag in data replication should be clearly visible in dashboard and alerts of same should be sent to respective authorities.

o. The Bidder shall be responsible for provisioning of bandwidth for replication of data between the DC site and DR Site. Geographical Location of the Disaster Recovery Environment shall be different location from the Data Centre environment or at a different place other than the Primary DC based on the project requirements. The DR/BCP setup configuration is required to be completed within 15 days from the project kick-off date during which the portal shall continue to be in operation.

11 **Monitoring of Cloud Services:** The bidder shall be responsible to monitor the cloud services and provide monitoring portals for complete infrastructure and services procured by DTAP.

12 **Interoperability support:** Bidder shall provide inter-operability support with regard to APIs and Data Portability.

13 **Security:** Bidder shall be responsible for security of resources, Network infrastructure along with implementation of security compliances. The DC/DR shall be equipped with state-of-the art physical, logical and network security solutions, appliances and equipment including surveillance, monitoring and management platforms and should be able to be monitored by a monitoring tool with facility to raise alerts in form of SMS, email & incident ticket. The DC and DR shall be physically located only in India. The Bidder must provide self-certification in this regard. Also, the bidder should provide the Cloud service offering facility of security management, monitoring of various devices/tools such as firewall, intrusion prevention/detection, content filtering and blocking, virus protection, event logging & correlation and vulnerability protection through implementation of proper patches and rules. Bidder shall notify DTAP promptly in the event of security incidents or intrusions, or any request to access data, to enable DTAP to manage these events proactively. The Bidder shall report forthwith in writing of information security breaches to the Department by unauthorized persons (including unauthorized persons who are employees of any Party) either to gain access to or interfere with the Project's Data, facilities or Confidential

Information. The Bidder also undertakes to treat information passed on to them under this Agreement as classified. Such Information will not be communicated /published / advertised by the Bidder to any person/organization without the express permission of the Department.

14 **Documentation:** Bidder shall provide necessary technical documentations, design documentations, standard Operating Procedures (SOPs) required for operations and management of services.

15 **Risk management**: All risk management related to migration; migration plan shall be worked out with NIC.

16 **Assessment of future needs:** The bidder shall asses the future needs of IFMIS application in coordination with NIC and DTAP.

17 **Reporting:** The bidder shall provide necessary details including sizing, current loads, utilization, expected growth/demand and other details for scale up/scale down on monthly basis. The bidder shall provide the relevant reports, including real time as well as past data/reports on dashboard. Also, bidder will be responsible to send daily status reports and ad hoc reports as required by the Purchaser.

18 **Dashboard:** The bidder will provide the dashboard for monitoring and financial aspects asper the bid document requirement. Bidder will also provide portal logins for billing, provisioning, usage etc. as per the requirement of the projects.

19 **DR Drills:** Bidder shall be responsible for conducting business continuity/DR drills. Bidder has to follow Standard Operating Procedures (SOP) and inform DTAP in advance for such drills which will have to be conducted two times a year, with 15 days' prior notice.

20 **Optimization of resources:** Bidder will optimize the resources/manage services for optimum billing with satisfactory service and provide report on utilization and optimization of the resources.

21 **Transition**: In case of change of CSP, the bidder will assist and support to ensure transfer of data from existing CSP to new CSP covering all required activities such as encryption of the data prior to transport and then decrypt it upon arrival.

22 **Backup:** The bidder shall ensure the regular (on daily basis) and scheduled backup of the entire set up including application, database and files. The bidder will also be required to set up cold backup facility on Tape drives at Finance Data Center or State Data Center. Necessary hardware will have to be provided by the selected bidder.

23 **Compliance:** The environment of Cloud shall comply with the respective empanelment compliance requirements published by Ministry of Electronics Information and Technology, Government of India.

24 **Malware Websites:** The Provider must provide Proactive and Request based takedown of Phishing, Malware websites, Fake Social Media Accounts, Mobile Applications, Advertisements etc

25 **Monitoring of Phishing: 24x7x365** proactive monitoring of World Wide Web etc. for Phishing, Brand Abuse, rogue apps and any other threat or exploitation which lead to compromising of credentials of the users of the department.

26 **Cloud Service Provisioning Requirements:**

a. Bidder should enable the Purchaser to provision / change cloud resources from application programming interface (API).
b. The user admin portal should be accessible via secure method using SSL certificate
c. The Purchaser should be able to take snapshot of virtual machines from provisioning portal.
d. The Purchaser should be able to size virtual machine and select require operating system when provisioning any virtual machines.
e. The Purchaser should be able to predict its billing of resources before provisioning any cloud resources.
f. The Purchaser should be able to set threshold of cloud resources of all types of scalabilities.
g. The Purchaser should be able to provision all additional storages required for cloud services.
h. The Purchaser should be able to provision any kind of resources either static or elastic resources.
i. The Purchaser should get list of all cloud resources from provisioning portal.
j. The Purchaser should be able to set the scaling parameters like in case of horizontal scaling,

k. The Purchaser should be able to set percentage / quantity of RAM consumption to trigger new virtual machines.
l. The Purchaser should be able to set percentage / quantity of network bandwidth to trigger new virtual infrastructure.
m. The Purchaser should be able to set port on which horizontal scaling will work. Port refers to be service port (such as port 80, 443) which should not change in case of horizontal scaling.
n. The Purchaser should be able to set minimum and maximum number of virtual machines which will be automatically provisioned as part of horizontal scaling to handle spike in load.

27 **Training:** Selected Bidder should provide cloud training/certification to DTAP nominated officials/personnel on usage of the Console and any other technical aspect for monitoring of IFMIS project in cloud. The Bidder will also train and transfer the knowledge to the replacement agency or NIC Data Center to ensure continuity and performance of services post expiry of Contract. Additionally, the bidder must provide training and certification for the NIC DC Team on Cloud Operations, network, security, Database, Application Performance Management (APM), Log Analytics, General Analytics Services, Active Directory Services, and WSUS Services in cloud

28 **Manpower:** Bidder shall provide 1 Cloud Support Engineer offsite throughout the contract period to support DTAP & NIC application team.

29 **Bidders must note that:** The DTAP requires essential security measures at the perimeter, network, and workload levels to protect against potential threats. These security measures should provide the capability to detect and mitigate known, unknown, and undisclosed threats from both external and internal sources. If possible, the department would prefer a single platform or security OEM that can meet these requirements. Additionally, the solution provider must have a datacenter located in India and must not share any data outside of Indian borders for any reason. Selected bidder must also ensure that:

1. The infrastructure provisioned by the Bidder must be scalable and shall allow DTAP to add/reduce cloud resources on demand basis through a user-friendly dashboard.
2. The portal/ application operations are secure and free from cyber-attacks, 24X7 proactive monitoring, protection against hacking and cyber-crimes. Thus, bidder will be responsible to provide “Safe to Host” certificate initially and then at periodic intervals of every 6 months.
3. Provided DC/DR’s core infrastructure is highly secured, managed covering the operational, computing infrastructure consisting of Hardware (Servers, Routers, Switches, and Networking Equipment), Operating Systems and associated Software (as middleware / application server software, database etc.), Internet Leased Lines with failover/redundancy).
4. The proposed cloud solution should have features like expand, scale up or scale out, horizontal & vertical scaling, upgrade the resources (virtual) including but not limited to Processors, Memory, Storage, Internet bandwidth, on the fly. Bidder’s needs to comply with these specifications and quantities mentioned in here. However, Bidders at their interpretations can propose infrastructure over and above this minimum specification as per project’s requirement.
5. There is adequate Internet Bandwidth for all portals / websites /applications hosted in the DC with SLA for availability, accessibility, security and response time and latency.
6. DTAP and its appointed third-party auditors may visit the Bidder DC /DR for auditing. The Bidder shall provide assistance and furnish the relevant information requested by the auditors.
7. No freeware software to be used unless authorized by DTAP.
8. Provided Cloud service has the facility of self-service portal for self-provisioning of cloud services like compute (Virtual, Docker, Containers, Database), file storage, object storage, caching (CDN, Memory Caching), networking (API Gateway, Load Balancer, NAT Gateway), etc within 5 minutes.
9. The bidder is expected to propose a solution for setting up a cloud infrastructure that aligns with the existing setup of the NIC Data Center.

8. ***Responsibility Matrix***

The Responsibility Matrix showing the responsibility of Bidder, Application vendor (NIC) and DTAP is placed below:-

Sl No.	Activity	CSP/MSP	Application vendor (NIC)	DTAP
1.	Understanding Application Architecture (Existing /New)	▨	▨	
2.	Design of Cloud Solution according to application	▨		
3.	Procurement of additional user Software licenses and installation according to application	▨		
4.	Installation of Application Software /Web portal/ Web Application	▨		
5.	Installation and updating the Operating Systems	▨		
6.	Installation and updating the Databases	▨		
7.	Installation and updating the middleware (if any)	▨		
8.	Configuration of Cloud Solution DC & DR	▨		
9.	Provisioning of the required hardware for Cloud	▨		
10.	Network Connectivity between DC and the DR site	▨		
11.	Internet Connectivity provisioning DC and the DR site	▨		
12.	Migration of application from existing environment setup to cloud	▨	▨	
13.	Infrastructure Testing	▨		
14.	Data Integrity Testing	▨		
15.	Cloud Solution Functional Testing	▨	▨	▨
16.	Switch Over Testing (Cloud to DR)	▨		
17.	Switch Over Testing (DR to Cloud)	▨		
18.	Cloud Solution Maintenance	▨		
19.	Cloud Service Provisioning through Self Service Portal /API	▨		

Sl No.	Activity	CSP/MSP	Application vendor (NIC)	DTAP
20.	24x7x365 Support, Cloud service Provisioning, de- provisioning, up-dation, auto-scaling etc.	▨		
21.	Maintenance & Management of Cloud Solution & infrastructure post implementation	▨		

9. SERVICE LEVEL AGREEMENT

9.1 General

The purpose of this Service Level Agreement (hereinafter referred to as SLA) is to clearly define the levels of service that shall be provided by the MSP to the DTAP and other stakeholders for the duration of the Project Term.

SLAs shall become part of agreement between the DTAP and the MSP. SLAs define the terms of the MSP's responsibilities in ensuring the timely delivery of the deliverables and the correctness of the same based on the agreed performance indicators as detailed in this section. The MSP has to comply with service level requirements to ensure adherence to project timelines, quality, functionality and availability of solution.

Penalty shall not be levied in the following cases:

- There is a Force Majeure event affecting the SLA which is beyond the control of the MSP.
- The non-compliance to the SLA is due to reasons beyond the control of the MSP.
  Note:
- Theft cases, by default, would not be considered "beyond the control of MSP". However, in certain cases, based on circumstances and certain locations, the DTAP may agree to qualify as "beyond the control of MSP". The same may be mutually agreed and signed between the MSP and the DTAP.
- MSP is also required to note that in case of SLA non-compliance considered as "beyond the control of MSP", the MSP would still need resolve the issue as per resolution SLAs of Critical/ High/ Medium/ Low Priority level incidents.

Definitions

For the purposes of this service level agreement, the following definitions and terms shall have meaning as tabulated below:

#	Term	Definition
a.	Uptime	Shall mean the time period for the specified services / components with the specified technical service standards are available to the users. Uptime, in percentage, of any component (Non-IT and IT) can be calculated as: Uptime = {1- [(Downtime) / (Total Time – Scheduled Maintenance Time)]} * 100
b.	Downtime	Shall mean the time period for which the specified services / components with specified technical and service standards are not available to the user department and excludes downtime owing to Force Majeure & Reasons beyond control of the MSP.
d.	Incident	Refers to any event/abnormalities in the functioning of the Services specified as part of the Scope of Work of the MSP that may lead to disruption in normal operations of the system.
e.	Response Time (For Incidents)	Shall mean the time elapsed from the moment an incident is reported in the Helpdesk, over phone or by any applicable mode of communication, to the time when a resource is assigned for the resolution of the same.

#	Term	Definition
g.	Resolution Time (For Incidents)	Shall mean the time taken (after the incident has been reported at the helpdesk) in resolving i.e. diagnosing, troubleshooting and fixing the reported incident
k.	Business hours	10am to 6pm on all days except non-working days
l.	Days	All Working and Non-Working days (365 days in a calendar year)
m.	24*7	Three shifts of 8 hours every day, this is applicable for all seven days of the week without any non-working days
n.	Scheduled Maintenance Time	The time that the System is not in service due to a scheduled activity as defined in this SLA. Further, scheduled maintenance time is planned downtime taken after permission of DTAP.
o.	Scheduled operation time	The scheduled operating hours of the System for the month. All scheduled maintenance time on the system would be deducted from the total operation time for the month to give the scheduled operation time. The total operation time for the systems and applications will be 24X7X365 (per year).
r.	QAP (Quarterly Amount Payable)	Amount towards Milestone achieved -
s.	QHIC (Quarterly Hosting Infrastructure Cost)	Amount towards Hosting Infrastructure Cost

9.2 SLA Framework

This section describes the SLA framework for this contract comprising of the following:

- Responsibilities of MSP
- Reporting procedures
- Issue management procedures
- Management escalation and contact map
- Measurement of SLA & Penalty

9.2.1 Responsibilities of MSP

The responsibilities of MSP are:

- MSP is responsible for delivering the services described in scope of work as per the service levels detailed in this document.
- Additionally, MSP is responsible for:
  - Reporting problems to the DTAP as soon as possible
  - Enable the DTAP to monitor the SLA
  - Providing early warning of any organizational, functional or technical changes that might affect MSP's ability to deliver the services described in the SLA
  - Resolve the production incidents in a timely manner

- Immediate action will be taken to identify problems and follow up with appropriate action to fix identified and those reported issues as quickly as possible.
- Overall coordination with DTAP for effective implementation

9.2.2 Reporting Procedures

The MSP's representative will prepare and submit SLA performance reports in an agreed upon format by the 7th working day of subsequent month of the reporting period. In addition to the monthly report MSP is responsible for generating reports as and when required by DTAP. The reports will include "actual versus target" SLA performance, a variance analysis and discussion of appropriate issues or significant events.

9.2.3 Issue Management Procedures

- This process provides an appropriate management structure for the orderly consideration and resolution of business and operational issues in the event that quick consensus is not reached between DTAP and MSP. It is expected that this pre-defined process will only be used on an exception basis if issues are not resolved at lower management levels.
- Either DTAP or MSP may raise an issue by documenting the business or technical problem, which presents a reasonably objective summary of both points of view and identifies specific points of disagreement with possible solutions.
- DTAP and the MSP's representative will determine which committee or executive level should logically be involved in resolution. A chain of management escalation is defined in next section.
- A meeting or conference call will be conducted to resolve the issue in a timely manner. The documented issues will be distributed to the participants at least 24 hours prior to the discussion if the issue is not an emergency requiring immediate attention.
- Management of DTAP and MSP will develop a temporary, if needed, and the permanent solution for the problem at hand. The MSP will then communicate the resolution to all interested parties.

  • In the event a significant business issue is still unresolved, the arbitration procedures described in the Contract will be used.

9.2.4 Management Escalation Procedures and Contact Map

- The purpose of this escalation process is to provide a quick and orderly method of notifying both parties that an issue is not being successfully resolved at the lower management level. Implementing this procedure ensures that DTAP and MSP's management are communicating at the appropriate levels.
- Escalation should take place on an exception basis and only if successful issue resolution cannot be achieved in a reasonable time frame.
- Either DTAP or MSP can initiate the procedure
- The "moving party" should promptly notify the other party that management escalation will be initiated
- Escalation will be one level at a time and sequentially

  • Dedicated /toll Free Telephone No. for Service Support: BIDDER/OEM must have Dedicated/toll Free

  • Escalation Matrix for Service Support: Bidder/OEM must provide Escalation Matrix of Telephone Numbers for Service Support.

- Management escalation will be defined as shown in the contact map below:

Stakeholder	Level	Name	Designation	Contact
DTAP	**L1**		Deputy Director	0771-2331305
	L2		Additional Director	0771-2331305
	L3		Director	0771-2331305
MSP	**L1**			
	L2			
	L3			

9.2.5 Measurement of SLA

The SLA metrics specify performance parameters as baseline performance, lower performance, and breach. All SLA calculations will be done on Monthly basis. The SLA also specifies the applicable penalty for lower performance and breach conditions. Payment to the MSP is linked to the compliance with the SLA metrics.

The SLA parameters shall be measured as per the individual SLA parameter requirements and measurement methods, through appropriate SLA Measurement tools to be provided by the MSP and approved and audited by DTAP for accuracy and reliability.

MSP shall provide the necessary tools required to measure the SLA parameters mentioned in this Agreement. The MSP shall be generating monthly SLA reports to DTAP. DTAP may appoint a Third-Party Agency to audit the performance, accuracy and integrity of the tools generating SLA data and also review the monthly SLA reports for SLA penalty computation. The DTAP shall also have the right to conduct, either itself or through any other agency as it may deem fit, an audit/revision of the SLA parameters. The SLAs defined, shall be reviewed by the DTAP on an annual basis after consulting the MSP, Project Management Consultants if any, and other experts. All the changes would be made by the DTAP post consultation with the MSP and might include some corrections to reduce undue relaxation in Service levels or some corrections to avoid unrealistic imposition of penalty, which are noticed after project has gone live.

Total penalty to be levied on the MSP shall be capped at 10% of the contract value. The DTAP would have right to invoke termination clause of the contract in case the overall penalty equals or exceeds 10% of contract value. If SLA penalty calculations exceed 15% of the quarterly payment for two consecutive quarters or 25% in any quarter, then DTAP may take appropriate action including termination of the contract and invoking the Performance Bank Guarantee.

9.2.6 Categories of SLA

Category	SLAs
Key Milestones	Attainment of key milestones on a timely basis
Hosting	Availability of Regular Reports

Category	SLAs
	Availability of all cloud services (based on revise Bill of Quantity submitted monthly by MSP)
	Recovery Time Objective (RTO)
	Recovery Point Objective (RPO)
	Application Performance
Manpower Deployment	Replacement/ Non-Availability of Acceptable Resource (Applicable for deployed resources at onsite)
Helpdesk	Helpdesk Incident Response Time Helpdesk Incident Resolution Time
	Helpdesk Re-opened Incidents
Miscellaneous	Project Management Report

9.2.7 Category-I: Key Milestones

Definition	Details
Service Level Requirement	Achievement of key milestones on-time on or before the deadline as mentioned in the contract without delay.
Measurement of Service Level Parameter	To be measured in number of weeks of delay (or part thereof) from the timelines mentioned in the subsection titled "Implementation approach and Plan"
Penalty for Non-achievement of SLA Requirement	Any delay in the delivery of the project milestones would attract a Penalty of 0.5% of the contract value per week (or part thereof) from the due date.

9.2.8 Category-II: Hosting

9.2.8.1 Availability of Regular Reports

Definition	**Details**
Service Level Requirement	Availability of Regular Reports (Cloud Services Consumption, Monitoring, Security, & Project Progress) indicating the compliance to the Requirements
Measurement of Service Level Parameter	Regular reports should be submitted to the DTAP within 5 working days from the end of the month over email/ hardcopy submission.
Penalty for Non-achievement of SLA Requirement	Penalty as indicated below (per occurrence): • <11 working days to >= 6 working days – 0.25% of QHIC (Quarterly Hosting Infrastructure Cost)

Definition	Details
	• <16 working days to >= 11 working days – 0.5% of QHIC (Quarterly Hosting Infrastructure Cost) • For the delay beyond 15 days - 1% of the QHIC (Quarterly Hosting Infrastructure Cost)

9.2.8.2 Availability of all cloud services

Definition	Details
Service Level Requirement	Availability be measured for each of the underlying components (e.g. VM, Storage, OS, VLB, Security Components) provisioned in the cloud. Measured with the help of SLA reports provided by CSP
Measurement of Service Level Parameter	Availability for each of the provisioned resources should be more than 99.5%
Penalty for Non-achievement of SLA Requirement	• >= 99.5%: No Penalty • For every 1% drop (or part thereof) below 99.5%, 0.25% of QHIC (Quarterly Hosting Infrastructure Cost) per component Note: In case the services are not available for a continuous period of 8 hours on any calendar day, penalty shall be 100% of the QHIC (Quarterly Hosting Infrastructure Cost) of the project.

9.2.8.3 Recovery Time Objective (RTO)

Definition	Details
Service Level Requirement	Measured during the regular planned or unplanned (outage) changeover from DC to DR or vice versa
Measurement of Service Level Parameter	RTO as defined in RFP
Penalty for Non-achievement of SLA Requirement	•0.1% of QHIC (Quarterly Hosting Infrastructure Cost) per every additional 1 (one) hour of downtime

9.2.8.4 Recovery Point Objective (RPO)

Definition	Details
Service Level Requirement	Measured during the regular planned or unplanned (outage) changeover from DC to DR or vice versa
Measurement of Service Level Parameter	RPO as defined in RFP
Penalty for Non-achievement of SLA Requirement	• 0.25% of QHIC (Quarterly Hosting Infrastructure Cost) per every additional 1 (one) hour of data loss

9.2.8.5 Application Performance

Definition	Details
Service Level Requirement	Percentage of transactions meeting the prescribed Target Response Time for Business Transactions for all components
Measurement of Service Level Parameter	Response Time would be calculated as time elapsed between sending a request from client to server and receiving the response. Response time of services to be measured at an interval of 30 minutes and averaged monthly on a quarterly basis.
Penalty for Non-achievement of SLA Requirement	**For all components (5 seconds)** • >= 99.95%: No Penalty • < 99.95% and >=95%: 0.05% of QAP per component • <95%: 0.1% of QAP per component

9.2.8.6 Security breach including Data Theft/Loss/Corruption /Malware Attack/Ransomware/ Denial of Service Attack/ Intrusion or defacement

Definition	Details
Service Level Requirement	Any incident wherein system including all cloud-based services and components are compromised or any case wherein data theft occurs (includes incidents pertaining to MSP only)
Measurement of Service Level Parameter	This penalty is applicable per incident. For each breach/data theft, penalty will be levied as per following criteria.

Definition	Details
Penalty for Non-achievement of SLA Requirement	For each breach/data theft, penalty will be levied as per following criteria. • Severity 1 - Penalty of Rs 15 Lakh per incident • Severity 2 - Penalty of Rs 10 Lakh per incident • Severity 3 - Penalty of Rs 5 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, DTAP reserve the right to terminate the contract and proceed with the legal action with the Jurisdiction district court, Raipur. For the purpose of this service level, the definition of severity is described as follows: Severity 1: Environment is down, or major malfunction resulting in an inoperative condition or disrupts critical business functions and requires immediate attention. A significant number of end users (includes public users) are unable to reasonably perform their normal activities as essential functions and critical programs are either not working or are not available 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 Severity 3: Moderate loss of performance resulting in multiple users (includes public users) impacted in their normal functions.

9.2.9 Category-III: Manpower

9.2.9.1 Replacement/ Non-Availability of Acceptable Resource (Applicable for Key Manpower Personnel)

Definition	Details
Service Level Requirement	At all times the SI should have required resource deployed on the project as per the requirements of RFP
Measurement of Service Level Parameter	In case MSP is not able to provide proposed resource or approved replacement of resource in a timely manner. Upon replacement of resource, the number of days for which a position remains vacant due to unavailability of resource acceptable to DTAP.

Definition	Details
Penalty for Non-achievement of SLA Requirement	• Delay in deployment of resources: INR 1,00,00 per resource per week (or part thereof) • Non-availability on working days without DTAP approval: INR 5,000 per resource per day • Every replacement of key resource (except when initiated on DTAP request): INR 50,000 per replacement

9.2.10 Category-IV: Helpdesk

9.2.10.1 Helpdesk Incident Response Time

Definition	Details
Service Level Requirement	95% of the tickets must be responded to within 30 minutes of receipt
Measurement of Service Level Parameter	Percentage of incidents acknowledge and respond once a ticket/incident is logged through any of the agreed channels. This is calculated for all tickets/incidents reported within the reporting quarter. For purpose of calculation, the percentage will be rounded-off.
Penalty for Non-achievement of SLA Requirement	>=95%: No Penalty <95%: 1% of QAP per one-percentage drop below the target of 95%

9.2.10.2 Helpdesk Incident Resolution Time

Definition	Details
Service Level Requirement	100% of the incidents should be resolved within prescribed time limit of problem reporting
Measurement of Service Level Parameter	Shall mean the time taken (after the incident has been reported at the IT helpdesk) in resolving i.e. diagnosing, troubleshooting and fixing the reported incident.

Definition	Details
Penalty for Non-achievement of SLA Requirement per incident	**Severity 1 (High)** • <=8 hours (No delay): No Penalty • >8 hours: For each 30 minutes of delay, 0.1% of QAP **Severity 2 (Medium)** • <=16 hours (No delay): No Penalty • >16 hours: For each 2 hours of delay, 0.05% of QAP **L1 – Severity 3 (Low)** • <=24 hours (No delay): No Penalty • >24 hours: For each 8 hours of delay, 0.03% of QAP

9.2.10.3 Helpdesk Re-opened Incidents

Definition	Details
Service Level Requirement	For all incidents which are designated resolved by the MSP,but are reopened by the client. This is calculated for all incidents reported within the quarter.
Measurement of Service Level Parameter	For purpose of calculation, the percentage will be rounded-off.
Penalty for Non-achievement of SLA Requirement	• <=2%: No Penalty • >2%: 1% of QAP per one-percentage drop below the target of 2%

9.2.11 Category-V: Miscellaneous

9.2.11.1 Project Management Report

Definition	Details
Service Level Requirement	Till go-live, the monthly reports are required to be submitted by the MSP. After go-live, the quarterly reports are required to be submitted by the MSP. These reports should be submitted within prescribed time-limit as follows: • On or before the 7th of next month (Monthly Report) • On or before the 15th of next month (Quarterly Report)
Measurement of Service Level Parameter	For purpose of calculation, the percentage will be rounded-off.

Definition	Details
Penalty for Non-achievement of SLA Requirement	• Monthly Reports: Rs. 50,000 (Fifty thousand) per incident of delay per week (or part thereof) • Quarterly Reports: Rs. 1,00,000 (One-Lakh) per incident of delay per week (or part thereof)

10. EXIT MANAGEMENT

Following are the responsibility of the MSP during Exit Management: -

- Assist the Department in migrating the VMs, data etc., and should ensure destruction of data
- Migration of the VMs, data, content and any other assets to the new environment or on alternate CSP's offerings and ensuring successful deployment and running of the Government Department's solution on the new infrastructure by suitably retrieving all data, scripts, software, virtual machine images, and so forth to enable mirroring or copying to Department supplied industry standard media.
- The format of the data transmitted from the CSP to the Department should leverage standard data formats (e.g., OVF, VHD...) whenever possible to ease and enhance portability.
- 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 Govt. Department / Agency.
- Ensure that all the documentation required for smooth transition including configuration documents are kept up to date
- Ensure that the CSP does not delete any data at the end of the contract (for a minimum of 45 days beyond the expiry of the contract) without the express approval of the Government Department / Agency. If data is to be retained the cost for retaining the data may be obtained in the commercial quote.
- Once exit process is completed, remove the data, content and other assets from the cloud environment and destroy the VM, content and data of the Govt. Department / Agency as per stipulations & shall ensure that data cannot be forensically recovered.
- Provide a comprehensive exit management plan.
- Carry out the migration of the VMs, data, content and any other assets to the new environment created by the Government Department / Agency or any other Agency (on behalf of the Department) on alternate CSP's offerings to enable successful deployment and running of the Government Department's solution on the new infrastructure.
- Address and rectify the problems with respect to migration of the Government Department / Agency application and related IT infrastructure during the transition.
- Ensure that all the documentation required by the Government Department / Agency for smooth transition (in addition to the documentation provided by the CSP) are kept up to date and all such documentation is handed over to the Government Department / Agency during regular intervals as well as during the exit management process.
- Support and assist the Government Department / Agency for a period of Please Insert duration so that l the Government

  Department / Agency is able to successfully deploy and access the services from the new environment.

  Train and transfer the knowledge to the Replacement Agency (or Government Department / Agency) to ensure similar continuity and performance of the Services post expiry of the contract.

11. SCHEDULE OF REQUIREMENT

11.1 Unpriced Bill of Material (BOM)

11.1.1 Schedule-I Part A (Licenses Supply)

Following are the required additional licenses along with Managed Services required for **Data Center**

Sr	Component	Metric	Quantity
1	Oracle Database EE Edition	Processor	12
2	Partitioning	Processor	12
3	Oracle Tuning Pack	Processor	12
4	Oracle Diagnostic Pack	Processor	12

11.1.2 Schedule-I Part B (Cloud Services)

a. Following is the requirement for hardware's at **Data Center**

Cloud Service	Metric	Quantity
Oracle Database Cloud Service – (CSP Native Managed Service)	vCPU/Hour	64
Compute – CPU	vCPU/Hour	88
Compute – Memory	GB/Hour	352
Block Storage (Boot Volume for Servers)	Gigabyte Storage Capacity/Month	5120
Block Storage (Storage for data)	Gigabyte Storage Capacity/ Month	5120
Storage IOPS (50 IOPS/GB)	Performance Units/Gigabyte/ Month	51200
Database backup Service	Gigabyte Storage Capacity/Month	5120
Backup Storage (Object Storage)	Gigabyte Storage Capacity/Month	5120
Load Balancer Base	LB Hour	2
Load Balancer Bandwidth	Mbps/Hour	400
DNS Service	1M Queries	1
DNS Traffic Management	1M DNS Traffic Management Queries	1
Next Generation Network Firewall Service with IPS in HA	Instance/Hour	1
Web Application Firewall – Requests	1M Incoming Requests/Month	10

Cloud Service	Metric	Quantity
Web Application Firewall – Instance	Instance/Month	2
OS Management Service	Instance/Month	20
Cloud Audit Service	Instance/Month	20
Cloud Security Posture Management Solution	Instance/Month	20
Public IP	Instance/Month	20
Threat Intelligence	Instance/Month	20
Vulnerability Scanning Service	Instance/Month	20
Antivirus	Instance/Month	10
Outbound Traffic	GB/Month	10240

b. Following is the requirement for hardware's at **Disaster Recovery**

Cloud Service	Metric	Quantity
Oracle Database Cloud Service – (CSP Native Managed Service)	vCPU/Hour	16
Compute – CPU	vCPU/Hour	22
Compute – Memory	GB/Hour	88
Block Storage (Boot Volume for Servers)	Gigabyte Storage Capacity/Month	5120
Block Storage (Storage for data)	Gigabyte Storage Capacity/ Month	5120
Storage IOPS (60 IOPS/GB)	Performance Units/Gigabyte/ Month	51200
Load Balancer Base	LB Hour	2
Load Balancer Bandwidth	Mbps/Hour	400
DNS Service	1M Queries	1
DNS Traffic Management	1M DNS Traffic Management Queries	1
Next Generation Network Firewall Service with IPS in HA	Instance/Hour	1
Web Application Firewall – Requests	1M Incoming Requests/Month	10
Web Application Firewall – Instance	Instance/Month	2

Cloud Service	Metric	Quantity
OS Management Service	Instance/Month	20
Cloud Audit Service	Instance/Month	20
Cloud Security Posture Management Solution	Instance/Month	20
Public IP	Instance/Month	20
Threat Intelligence	Instance/Month	20
Antivirus	Instance/Month	10
Vulnerability Scanning Service	Instance/Month	20

Note:

1. The details mentioned in the bill of material are indicative and minimum only. The bidder must analyze the current architecture and existing set up of the application hardware and provide its unpriced BoM meeting the best suited solution for lifting and shifting the application over the cloud environment
2. Department has already specified the available database licenses with the database options to use the same for IFMIS applications. Bidders need to provision the database system as specified in the above table for DC & DR with BYOL options with existing available licenses. Bidder must need to comply database OEM licensing policy for BYOL. In case of any gap of license bidder need to procure the licenses to comply the infra requirement and OEM licensing policy. Please submit the relevant documentation (Public available URL/ Oracle Confirmation letter).

12. ***PRE-BID QUERIES SUBMISSION TEMPLATE***

This section has been deleted.

13. ANNEXURE I: PRE-QUALIFICATION BID TEMPLATES

13.1 Form-PQ1: Format for Cover Letter for Earnest Money Deposit

[To be submitted by the lead bidder on its letterhead]

[Cover Letter 1A]

To,

The Director, Directorate of Treasury, Account & Pension,
Government of Chhattisgarh,
1st Floor, A Block, Indravati Bhawan,
Nawa Raipur Atal Nagar, Chhattisgarh – 492101

1. In consideration of ________________ (hereinafter called "DTAP") represented by ________________, on the first part and M/s ____________ of ___________ (hereinafter referred to as "bidder") on the Second part, having agreed to accept the Earnest Money Deposit of Rs. ________ (Rupees _________) in the form of Bank Guarantee for the Request for Proposal for procurement of _________ we __________ (Name of the Bank), (hereinafter referred to as the "Bank"), do hereby undertake to pay DTAP forthwith on demand without any demur and without seeking any reasons whatsoever, an amount not exceeding ______ (Rupees _______) and the guarantee will remain valid up to a period of 225 days from the last date of the bid submission. It will, however, be open to DTAP to return the Guarantee earlier than this period to the System Integrator in case the System Integrator does not qualify to standards defined in different stages of the Bid mentioned in RFP as per the recommendation of the bid evaluation Committee (BEC) as constituted by DTAP.
2. In the event of the bidder withdrawing the tender before the completion of the stages prior to the Price negotiations or during the Price negotiations, as the case may be, the Guarantee deposited by the bidder stands forfeited to DTAP. We also undertake not to revoke this guarantee during this period except with the previous consent of DTAP in writing and we further agree that our liability under the Guarantee shall not be discharged by any variation in the term of the said tender and we shall be deemed to have agreed to any such variation.
3. No interest shall be payable by DTAP to the bidder on the guarantee for the period of its currency.

For and on behalf of (Bidder)

Signature:

(Authorized Signatory) Name of
the person:

Designation:

Company seal:

For the Bank of ___________________

(Agent/Manger)

13.2 Form-PQ2: Format for Power of Attorney to Authorized Signatory

POWER OF ATTORNEY

[To be executed on non-judicial stamp paper of INR 500/- and notarized. The stamp paper to be in the name of the company which is issuing the power of attorney.]

We, M/s.______ (name of the firm or company with address of the registered office) hereby constitute, appoint and authorize Mr. or Ms.______ (Name and residential address) who is presently employed with us and holding the position of ______, as our Attorney to do in our name and our behalf all or any of the acts, deeds or things necessary or incidental to the RFP for the Project <<Assignment Name>>, including signing and submission of the RFP response, participating in the meetings, responding to queries, submission of information or documents and generally to represent us in all the dealings with Client or any other Government Agency or any person, in connection with the works until culmination of the process of bidding till the Project Agreement is entered into DTAP and thereafter till the expiry of the Project Agreement.

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

Dated this the _____ day of ______ 2024

(Signature and Name of authorized signatory) ___________

(Signature and Name in block letters of all the remaining partners of the firm Signatory for the Company)

Seal of firm Company

Witness 1: Witness 2:

Note: The Mode of execution of the power of attorney should be in accordance with the procedure, if any laid down by the applicable law and the charter documents of the executant(s) and when it is so required the same should be under common seal affixed in accordance with the required procedure.

13.3 Form-PQ3: Pre-Qualification Bid Covering Letter

[Cover Letter 1B]

[To be submitted by the lead bidder on its letterhead]

Date: DD/MM/YYYY

To,
The Director, Directorate of Treasury, Account & Pension,
Government of Chhattisgarh,
1st Floor, A Block, Indravati Bhawan,
Nawa Raipur Atal Nagar, Chhattisgarh – 492101

Ref: Tender No. **<<….>> dated << ….>>**

Subject: Submission of the Pre-Qualification Bid for the referenced tender

Dear Sir,

With reference to your Request for Proposal for <<Assignment Name>>, we hereby submit our Pre-Qualification Bid for the same.

We hereby declare that:

a. We hereby acknowledge and unconditionally accept that the DTAP can at its absolute discretion apply whatever criteria it deems appropriate, not just limiting to those criteria set out in the RFP and related documents, in short listing of MSP for providing services.
b. We have submitted EMD of INR XXXX Crore via <<Mode of Payment>> and Tender fee of INR XXXX online.
c. We hereby declare that all information and details furnished by us in the Bid are true and correct, and all documents accompanying such application are true copies of their respective originals.
d. We agree to abide by our offer for a period of 180 days from the date of opening of prequalification bid prescribed by Authority and that we shall remain bound by a communication of acceptance within that time.
e. We have carefully read and understood the terms and conditions of the RFP and the conditions of the contract applicable to the RFP. We do hereby undertake to provision as per these terms and conditions.
f. In the event of acceptance of our bid, we do hereby undertake:
   - To supply the products and commence services as stipulated in the RFP document
   - To undertake the project services for entire contract period from the date of signing of the contract as mentioned in the RFP document.
   - We affirm that the prices quoted are inclusive of design, development, delivery, installation, commissioning, training, providing facility management and handholding support, and inclusive of all out of pocket expenses, taxes, levies discounts etc.
g. We do hereby undertake, that, until a formal contract is prepared and executed, this bid, together with your written acceptance thereof and notification of award of contract, shall constitute a binding contract between us.

h. We understand that the Authority may cancel the bidding process at any time and that Authority is not bound to accept any bid that it may receive without incurring any liability towards the bidder.
i. We fully understand and agree to comply that on verification, if any of the information provided in our bid is found to be misleading the selection process, we are liable to be dismissed from the selection process or termination of the contract during the project, if selected to do so

In case of any clarifications please contact ___________________ having email id____________and contact number________________.

Thanking you,

Yours sincerely,

(Signature of the Sole or Lead bidder)

Printed Name

Designation

Seal Date:

Place:

Business Address:

FORWARDING LETTER

From

(Full Name & Communication Address, Email, Mob. No., Website of the Bidder)
____
____

13.4 Form-PQ4: Compliance to Pre-Qualification Criteria

The pre-qualification proposal should comprise of the following basic requirements. The documents mentioned in this compliance sheet along with this form, needs to be a part of the Pre-Qualification proposal.

S. No.	Eligibility Criteria	Documentary proof to be submitted	Provided	Reference & Page Number
1	**Tender Fee**	Tender document fees of Rs.20,000/-is to be deposited by Demand Draft in the name of "Director Treasury Accounts and Pension" payable at Raipur. Upload the scanned copy of DD in e-procurement portal. Before opening the bid, original copy of DD must be submitted at the office of Director Treasury Accounts and Pension, Indravati Bhawan, First Floor, Block-A, Nawa Raipur, Atal Nagar, Chhattisgarh.		
2	**EMD**	a. EMD Amount of Rs.10,00,000/-is to be deposited by Demand Draft or through Challan/Challan in head 8443-103 in the name of "Director Treasury Accounts and Pension" payable at Raipur. b. Scanned copy of DD or challan/Challan (to be submitted along with bid) c. Before opening the bid, original copy of DD or e-Challan has to be submitted at the office of Director, Treasury Accounts and Pension, Indravati Bhawan, First Floor, Block-A, Nawa Raipur, Atal Nagar, Chhattisgarh.		

S. No.	Eligibility Criteria	Documentary proof to be submitted	Provided	Reference & Page Number
3	**Power of Attorney (PoA)**	Board Resolution, 'Power of Attorney to Authorize Signatory' (Format Specified in Annexure-I) a. Scanned copies of document to be submitted online on e-Procurement Portal b. Original document (to be submitted physically to communication address mentioned in Bid Control Sheet on or before the last date and time		
4	**Legal Entity**	a. Certificate of Incorporation of the Company/LLP b. Copy of PAN / TAN c. Copy of Registration Certificates with the GST Authority d. Copy of Income Tax and GST returns for last financial year (FY 2022-23 and FY 2021-22) (To be submitted in the format provided under Form – PQ 5)		
5	**Declaration for not being blacklisted *(as on Date of submission of bid)***	Self-Declaration by bidder on its letterhead as per Annexure I Form *(To be submitted in the format provided under Form – PQ 8)*		
6	**Insolvency / Bankruptcy**	Self-Declaration by bidder on its letterhead that company has not been declared insolvent/ bankrupt or should not have filed for insolvency/ bankruptcy or in the process of being declared bankrupt before any designated authority.		

S. No.	Eligibility Criteria	Documentary proof to be submitted	Provided	Reference & Page Number
7	**Average Annual turnover of MSP from Cloud Services or Data Center Establishment Services or IT Services**	Stamped Certificate from the Statutory Auditor/CA on turnover details from Cloud Services or Data Centre Establishment services or IT Services Work for the last three (3) financial years for which audited Financial statements are available. *(To be submitted in the format provided under Form – PQ 6)*		
8	**Annual Turnover**	CA Certificate and certified copy of turnover to be submitted.		
9	**Positive Net worth**	Certificate from the Statutory Auditor/CA on net worth in the last three (3) financial years for which audited financial statements are available. *(To be submitted in the format provided under Form – PQ 6)*		
10	**Experience with Government/PSU**	Work Order/ Completion certificate		
11	**MeitY empanelment**	Valid certificate from MeitY.		
12	**MAF from CSP**	Undertaking from CSP. MAF from CSP for Cloud Services and MAF for Oracle database Licenses.		
13	**Certifications**	Copy of valid certifications in the name of the CSP (valid on the date of bid submission)		

S. No.	Eligibility Criteria	Documentary proof to be submitted	Provided	Reference & Page Number
14	**Accreditations**	Third Party Audited/Applicable reports to be submitted.		
15	**Unit Price Listing**	Public URL and CSP Self Confirmation on CSP letterhead from authorized signatory		
16	**Technical Capability-Experience in Cloud/Data Center Infrastructure**	Work Order/ Contract/Self Declaration clearly highlighting the scope of work and value of the contract/ order		
17	**Relevant resources onboard**	Certificate by Human Resources Department of the bidder on bidder's letterhead.		

13.5 Form-PQ5: Details of Bidder Organization

<<To be printed on Bidder Company's Letterhead and signed by Authorized Signatory>>

Date: DD/MM/YYYY
To,
The Director, Directorate of Treasury, Account & Pension,
Government of Chhattisgarh,
1st Floor, A Block, Indravati Bhawan,
Nawa Raipur Atal Nagar, Chhattisgarh – 492101

Subject: Bidder Organization Details

Ref: Tender No. **<<….>> dated << ….>>**

Dear Sir,

Please find below details of Bidder for participation in tender floated for selection of MSP for hosting, commissioning, data migration and O&M of e-Kosh application on cloud environment

Bidder Information Sheet

#	Particulars	Bidder
1.	Name and address of the bidding Company	
2.	Incorporation status of the firm (Pvt. Ltd./Public Limited/LLP)	
3.	Year of Establishment	
4.	Country of Registered Office	
5.	Address of Registered Office	
6.	Company Registration Details	
7.	Date of Registration	
8.	Details of any Certifications (ISO etc.)	
9.	GST Number	
10.	PAN/Equivalent	
11.	TAN/Equivalent	
12.	Authorized Signatory Name	
13.	Authorized Signatory Designation	

#	Particulars	Bidder
14.	Authorized Signatory Contact Details Name, Address, email, Phone nos. and Mobile Number of Contact Person	

Yours sincerely,

Signature of Authorized Signatory (with official seal)

Name:

Designation:

Address:

Telephone & Fax:

E-mail Address:

13.6 Form-PQ6: Annual Turnover and Net Worth

<< To be printed on Statutory Auditor's Letterhead with stamped and signed by Authorized Signatory>>

Date: DD/MM/YYYY

To,

The Director, Directorate of Treasury, Account & Pension,
Government of Chhattisgarh,
1st Floor, A Block, Indravati Bhawan,
Nawa Raipur Atal Nagar, Chhattisgarh – 492101

Subject: Request for Proposal for <<Assignment Name>>
Ref: Tender No. <<…..>> dated << …..>>
Dear Sir,
I have carefully gone through the Terms & Conditions contained in the RFP document for <<Assignment Name>>. I hereby declare that below are the details regarding Turnover and Net-worth for our organization for last 3 financial years:

Financial Year	Overall Turnover	Turnover as per <<pre-qualification criteria>>	Net-Worth
F.Y. 1 (in INR Crore)			
F.Y. 2 (in INR Crore)			
F.Y. 3 (in INR Crore)			
Average			

Note: Latest three FY for which audited FY statements are available.

Contact details of officials for future correspondence regarding the bid process:

Details	Authorized Signatory	Secondary Contact
Name		
Title		
Company Address		
Mobile		
Email		

I further certify that I am competent officer in my company to make this declaration.

Yours sincerely,

____

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

13.7 Form-PQ7: Format for Bidder’s Experience

Sl no	**Name of the Client Served**	**Nature of the Work/Services Provided**	**Contract Period**		**Value of the Contract**	**Financial year of execution of work**	**Value of the Work executed against Col no.**
			From	To			

For Example

Sl no	**Name of the Client Served**	**Nature of the Work/Services Provided**	**Contract Period**		**Value of the Contract**	**Financial year of execution of work**	**Value of the Work executed against Col no.**
			From	To			
1	XYZ	Cloud Services	01.10.2018	30.09.2021	300 lacs	2018-19	50 lacs
						2019-20	100 lacs
						2020-21	100 lacs
						2021-22	50 lacs

Note: All requisite documents as specified in Bidder qualification in support of experience shall be submitted.

Authorized Signatory with Seal

13.8 Form-PQ8: Undertaking of not being Blacklisted

<<To be printed on Bidder Company's Letterhead and signed by Authorized Signatory>>

Date: DD/MM/YYYY
To,
The Director, Directorate of Treasury, Account & Pension,
Government of Chhattisgarh,
1st Floor, A Block, Indravati Bhawan,
Nawa Raipur Atal Nagar, Chhattisgarh – 492101

Subject: Declaration for not being debarred/ black-listed by Central/ any State Government department/ Public Sector Undertakings in India as on the date of submission of the bid

Ref: Tender No. <<….>> dated << …...>>

Dear Sir,

I/We, the undersigned, herewith declare that in the last three years, my company (<-- name of the firm ->) has not been debarred/ black-listed by Central Government Department, any State Government department, or Public Sector Undertakings of Central Government or State Government in India as on the date of submission of the bid.

For and on behalf of

Signature:

(Authorized Signatory) Name of
the person:

Designation:

Company seal:

13.9 Form-PQ9: No Deviation Certificate

<<To be printed on Lead Bidder Company's Letterhead and signed by Authorized Signatory>>

Date: DD/MM/YYYY

To,

The Director, Directorate of Treasury, Account & Pension,
Government of Chhattisgarh,
1st Floor, A Block, Indravati Bhawan,
Nawa Raipur Atal Nagar, Chhattisgarh – 492101

Ref: Tender No. **<<….>> dated << ….>>**

Subject: Certificate of No Deviation

This is to certify that our offer is exactly in consonance with your RFP no. _________ dated __________ and subsequent amendments / corrigendum's etc. This is to expressly certify that our offer contains no deviation on Technical (including but not limited to Scope of Work, Technical Requirements Specification, Operational and Infrastructure requirements of IFMIS as laid out in the RFP, Legal or Commercial aspects in either direct or indirect form.

Yours sincerely,

<Date>

<on behalf of Bidder Name>

Authorized Signature [In full and initials]:

Name and Title of Signatory:

Name of Firm:

Address:

Seal/Stamp of Bidder:

13.10 Form-PQ10: Total Responsibility

<<To be printed on Sole or Lead Bidder Company's Letterhead and signed by Authorized Signatory>>

Date: DD/MM/YYYY
To,
The Director, Directorate of Treasury, Account & Pension,
Government of Chhattisgarh,
1st Floor, A Block, Indravati Bhawan,
Nawa Raipur Atal Nagar, Chhattisgarh – 492101

Ref: Tender No. **<<….>> dated << ….>>**

Subject: Certificate of Total Resposibility

This is to certify that we [insert name of Sole or Lead Bidder company name] undertake the total responsibility for the defect free operation of the proposed solution as per the requirement of the RFP for the duration mentioned of the RFP.

Yours sincerely,

<Date>

<on behalf of Bidder Name>

Authorized Signature [In full and initials]:

Name and Title of Signatory:

Name of Firm:

Address:

Seal/Stamp of Bidder:

13.11 Form-PQ11: Undertaking for No Conflict of Interest

<<To be printed on Sole or Lead Bidder Company's Letterhead and signed by Authorized Signatory>>

Date: DD/MM/YYYY
To,
The Director, Directorate of Treasury, Account & Pension,
Government of Chhattisgarh,
1st Floor, A Block, Indravati Bhawan,
Nawa Raipur Atal Nagar, Chhattisgarh – 492101

Ref: Tender No. **<<….>> dated << ….>>**

Subject: Certificate for undertaking for No Conflict of Interest

We hereby confirm that our company <insert name of sole or lead company name> is not involved in any conflict-of-interest situation with one or more parties in this bidding process, including but not limited to –

- Receive or have received any direct or indirect subsidy from any of them; or
- Have common controlling shareholders; or
- Have the same legal representative for purposes of this Bid; or
- Have a relationship with each other, directly or through common third parties, that puts them in a position to have access to information about or influence on the Bid of another Bidder, or
- Influence the decisions of DTAP regarding this bidding process; or
- Participation in more than one bid in this bidding process. Participation in more than one Bid will result in the disqualification of all Bids. However, this does not limit the inclusion of the same product (commercially available hardware, software or network product manufactured or produced by the firm), as well as purely incidental services such as installation, configuration, routine training and ongoing maintenance/support, in more than one bid; or
- Participation as a consultant in the preparation of the design or technical specifications of the goods and services that are the subject of the bid.
- Association as Consultant / Advisor / Third party independent evaluating agency with any of the agencies taking part in the bid process.

Yours sincerely,
(Authorized Signatory)
(Name, Designation, Address, Contact Details, Seal, Date)

14. ANNEXURE II: TECHNICAL BID TEMPLATES

Bidder needs to submit the technical bid in the forms presented below.

14.1 Form-TQ1: Technical Bid Covering Letter

[Cover Letter 3]

[To be submitted by the lead bidder on its letterhead]

Date: DD/MM/YYYY
To,
The Director, Directorate of Treasury, Account & Pension,
Government of Chhattisgarh,
1st Floor, A Block, Indravati Bhawan,
Nawa Raipur Atal Nagar, Chhattisgarh – 492101

Kind Attn.: Director, DTAP

Subject: Submission of the Technical bid for selection of MSP/CSP for hosting, commissioning, data migration and O&M of e-Kosh application on cloud environment

Dear Sir,

We, the undersigned, offer to provide services for hosting, commissioning and data migration the e-kosh application with reference to your request for proposal bearing <insert RFP reference number> dated <insert date>. We are hereby submitting our Technical bid.

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

We agree to abide by all the terms and conditions of this RFP document. We would hold the terms of our proposal valid for the number of days as stipulated in the RFP document.

We understand you are not bound to accept any proposal you receive.

Yours sincerely,

(Authorized Signatory)

(Name, Designation, Address, Contact Details, Seal, Date)

14.2 Form-TQ2: Compliance Sheet for Technical Proposal

The below mentioned compliance sheets mandatorily need to be submitted by the bidder in their technical proposal on Cloud environment: -

Following are the compliance and reference documents for Submission of the Technical proposal for Selection of MSP for cloud services for IFMIS project against tender no <tender no.> dated <date>

Compute

#	Description	Compliance (Yes/No)	Reference
1	The CSP should provide the following instance types to choose from - • Virtual Machine • Bare Metal Instances • Dedicated Physical Server		
2	The proposed system should have facility to choose from various VMs shapes and sizes.		
3	CSP Should support per minute/hour billing option for Infrastructure - compute services		
4	The CSP should allow to choose between the different type of processors like Intel or AMD when creating a virtual machine.		
5	The CSP should offer an option of running customer's choice of hypervisor. The CSP should support 3 standard hypervisors KVM, Microsoft Hyper-V and VMware		
6	CSP shall support industry standard OS such as Windows and any 2 flavors of following Linux. Oracle Linux, Redhat Linux, Ubuntu & CentOS		
7	The CSP should ensure that underlying processors should not have been discontinued by the processor OEM at time of bidding.		
8	The CSP should provide a self-service provisioning, manage and terminate multiple VMsconcurrently either through a programmatic interface (i.e. API/CLI) or through a management console or Web Portal without involving the service provider.		
9	The proposed system should allow to configure policies to automatically increase/scale the number of Instances/VMs during demand spikes to maintain performance		
10	The CSP should allow dedicated hosts for Virtual machine instances.		
11	The CSP should be able to support the various enterprise Linux distributions.		

#	Description	Compliance (Yes/No)	Reference
12	The CSP should be able to support the major Windows Server versions.		
13	The platform should allow horizontal scaling of the instances without any outage. A maintenance window is allowed for vertical scale-up of VM to specify and modify server configuration (CPU, memory, storage) parameters.		
14	The platform must offer self-service provisioning of multiple instances concurrently either through a programmatic interface (API/CLI) or through a management console.		
15	The platform should allow logical grouping of instances together for applications that require low network latency and/or high network throughput or for maintenance operations.		
16	The platform service should allow to configure for automatic increase of number of instances during demand spikes to maintain performance and decrease capacity during lulls to reduce costs.		
17	The Cloud must support the ability to take an existing running instance or a copy of an instance and export the instance into a custom image format.		
18	The Cloud service should support containers, including Docker and/or other containerization platforms and should offer Manager Kubernetes as service.		
19	The Cloud provider should offer a managed highly scalable, high performance container management service.		
20	The Cloud service should be able to run customer code in response to events and automatically manage the compute resources.		
21	The Cloud provider should offer a simple pay-as-you-go pricing where customers can pay for compute capacity with no long-term commitments.		
22	CSP Shall provide the cloud native tools to monitor the performance of IT setup including the compute, memory, disk, I/Os bandwidth, application parameters and provisioned services.		
23	The CSP should allow logical segregation of resources into various groups for better management and billing purposes.		
24	Auto scaling of compute based on metrics (CPU & memory) & time/schedule based to align with business demand like month end peak, quarterly & annual peaks		
25	Flexible custom shape to enable number of vCPU's/ RAM (e.g. vCPU 2,4,6,8,10,12,14 etc) that will be need as per business workloads		

#	Description	Compliance (Yes/No)	Reference
26	Changing shape of a virtual machine (VM) instance without having to rebuild your instances or redeploy your applications, this bring agility & speed to business requirement		
27	Linux operating system should be able to automatically apply patches, updates and tune without human interaction.		

Block Storage

S.NO.	Description	Compliance (Yes/No)	Reference
1	Cloud provider should offer persistent block level storage volumes for use with compute instances.		
2	Cloud provider should offer block storage volumes supporting a size ranging from atleast 100 GB to 32 TB.		
3	Cloud service should support NVMe backed storage media that offer single digit millisecond latencies.		
4	Cloud 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.		
5	Cloud service should support encryption of data on volumes, disk I/O, and snapshots using industry standard AES-256 cryptographic algorithm.		
6	Cloud service should support encryption using customer managed keys.		
7	Cloud service should support point-in-time snapshots. These snapshots should be incremental in nature.		
8	Cloud Service should support sharing of backups/snapshots across regions making it easier to leverage multiple regions for geographical expansion, data centre migration, and disaster recovery.		
9	Cloud service should support attaching of storage volume to multiple compute instances in R/W mode so that users can access and share a common data source.		
10	Cloud service should support a baseline IOPS of atleast 60 IOPS/GB and maintain it consistently at scale		
11	Cloud service should support performance IOPS of 75 IOPS/GB and maintain it consistently at scale		

S.NO.	Description	Compliance (Yes/No)	Reference
12	Cloud service should be durable and support annual failure rates of less than 1%		
13	Cloud 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 to be available as expandable I/O		
14	Cloud service should support encryption of data on volumes, disk I/O, and snapshots using industry standard AES-256 cryptographic algorithm		
15	Cloud Service should support sharing of snapshots across regions making it easier to leverage multiple regions for geographical expansion, data center migration, and disaster recovery		
16	Should support resize your block/boot volumes without any downtime, which means you do not have to take down your application so there is no Downtime.		
17	Should support detached block volumes to the lower cost setting automatically and enable when ready to use them for your workloads by simply attaching them		
18	instantaneous storage performance customization to support elastic performance on demand, instantaneous, without a lengthy migration or downtime		

Object Storage

S.No	Description	Compliance (Yes/No)	Reference
1	Cloud provider should offer secure, durable, highly-scalable object storage for storing and retrieving any amount of data from the web.		
2	Cloud provider should support an extremely low-cost storage service that provides durable storage with security features for data archiving and backup.		
3	Cloud service should support encryption for data at rest using 256-bit Advanced Encryption Standard (AES-256) encryption to encrypt your data.		
4	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.		

S.No	Description	Compliance (Yes/No)	Reference
5	Cloud service should support encryption using a Key Management Service that creates encryption keys, defines the policies that control how keys can be used, and audits key usage to prove they are being used correctly.		
6	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.		
7	Cloud provider should provide a strong regional isolation, so that objects stored in a region never leave the region unless customer explicitly transfers them to another region.		
8	Cloud service should be able to send notifications when certain events happen at the object level (addition/deletion).		
9	Cloud Service should support versioning, where multiple versions of an object can be kept in one object storage account. Versioning protects against unintended overwrites and deletions.		
10	Cloud service should support flexible access-control policies to manage permissions for objects.		
11	Cloud service should be able to provide audit logs on storage account including details like Time the API activity occurred, Source of the activity, Target of the activity, Type of action and Type of response		
12	Cloud provider should offer a storage gateway appliance for seamlessly storing on-premises data to the cloud.		
13	Cloud service should support read-after-write consistency for PUT operations for new objects		

Network

S.No	Description	Compliance (Yes/No)	Reference
1	Support the ability to create a logical, isolated virtual cloud network that represents a company’s own network in the cloud		
2	Support connecting two virtual cloud networks within the same Region or across regions to route traffic between them using private IP addresses		
3	Offer the capability of creating fully isolated (private) subnets where Instances/VMs can be provisioned without any public IP address or Internet routing		

S.No	Description	Compliance (Yes/No)	Reference
4	Support multiple IP protocols, including TCP, UDP, and ICMP		
5	Cloud service should be able to support IP address ranges specified in RFC 1918 as well as publicly routable CIDR blocks		
6	Support the capability of automatically assigning public IP addresses to Instances/VMs		
7	Support Internet Protocol version 6 (IPv6) at the gateway and expose this functionality to users		
8	Support the ability to assign multiple IP addresses for a Network Interface Card (NIC) attached to a given Instance/VM		
9	Support the ability to assign multiple Network Interface Cards (NICs) to a given Instance		
10	Support adding or removing firewall rules applicable to inbound traffic (ingress) to Instances/VMs		
11	Support adding or removing firewall rules applicable to outbound traffic (Egress) from Instances/VMs		
12	Offer Network Access Control Lists (NACL) to control inbound and outbound traffic to subnets		
13	Offer the capability of capturing network traffic flow logs		
14	Provide a network address translation (NAT) gateway managed service to enable Instances/VMs in a private network to connect to the Internet, but prevent the Internet from initiating a connection to those Instances/VMs		
15	Provide a managed internal gateway service to enable Instances/VMs to connect to selective PaaS cloud services like Object storage for backup etc. This service should be separate from NAT gateway service		
16	Support IPSec VPN connectivity between the cloud provider and the customer's data center with No extra cost		
17	Support multiple IPSec Virtual Private Network (VPN) connections per Virtual Network		
18	Ability to make direct leased-line connections between the cloud provider and a user datacenter		
19	Offer a front-end (internet-facing) load balancing service that takes requests from clients over the Internet and distributes them across Instances/VMs that are registered with the Load Balancer		

S.No	Description	Compliance (Yes/No)	Reference
20	Offer a back-end (private) load balancing service that routes traffic to Instances/VMs hosted in private subnets		
21	Offer a Layer 7 (HTTP) Load Balancer service capable of load balancing network traffic across multiple Instances/VMs		
22	Offer a load balancing service that supports session affinity		
23	CSP should have expanded cluster networking capabilities by enabling remote direct memory access (RDMA)		
24	The backend network fabric should use Mellanox's or equivalent standards ConnectX-5, 100-Gbps network interface cards with RDMA over Converged Ethernet (RoCE) v2 to create clusters with 2 microsecond low-latency networking.		
25	CSP Network should have layer 3 DDoS capabilities natively available		
26	Virtual Cloud Network or cloud network should support view connection information for traffic within and to and from your virtual cloud network via logs to enable Troubleshooting and Monitoring.		
27	Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections		

Cloud Security

S.No	Description	Compliance (Yes/No)	Reference
1	CSP should offer a Web Application Firewall (WAF) that helps protect web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources		
2	CSP should offer WAF service with over 250 predefined OWASP, application and compliance-specific rules. The WAF should also provide aggregated threat intelligence from multiple sources, including Webroot Bright Cloud®. It should Integrate with CSP's Identity, Audit and Monitoring services for a cohesive approach.		

S.No	Description	Compliance (Yes/No)	Reference
3	CSP should offer WAF service in which administrators can add and configure their own access controls rules based on geolocation data, whitelisted and blacklisted IP addresses, and HTTP URL and header characteristics. It should Provide WAF protection for CSP's cloud deployments and across on-premises, hybrid cloud, and multi cloud environments		
4	THE CSP should offer WAF service which includes features that allow to detect and either block or allow identified bot traffic to web applications. Bot management features should include: JavaScript Challenge, CAPTCHA Challenge, and Good Bot whitelists		
5	Offer a service to protect from common, most frequently occurring network layer (Layer 3) Distributed Denial of Service (DDoS) attacks as a part of default virtual cloud network. It should not be separately charged		
6	Offer a service to protect from common, most frequently occurring application layer (Layer 7) Distributed Denial of Service (DDoS) attacks, along with the ability to write customized rules to mitigate sophisticated application layer attacks		
7	CSP should offer service which capture logs of all user activity within tenancy. The recorded information shall include identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the cloud service.		
8	Cloud provider should offer a service to record history of API calls and related events for a user account		
9	CSP should offer fine-grained access controls with authentication with a multi-factor authentication		
10	CSP should offer integration with On-premises Active Directory through Active Directory Federation services		
11	Cloud service should support features such as user and group management.		
12	CSP should have data encryption service to encrypt data while in transit or on-rest by default.		
13	CSP should offer a service with customer generated encryption key to create and control the encryption keys used to encrypt user data		
14	CSP Should offer Managed Key Management service which can store keys in a FIPS 140-2 Level 3 certified hardware security module		

S.No	Description	Compliance (Yes/No)	Reference
	(HSM).		
15	CSP should offer KMS Integration with CSP's Identity and Access Management (IAM) to control permissions on individual keys and key vaults, and monitor their lifecycle via integration with CSP's Audit service		
20	CSP should offer a logical container service to organize and control access to the cloud Resources (Compute, Storage, Network, Load Balancer etc.) created within that container with some policies, which restricts who can use the resources created within than container other than administrators of your account. The feature should support creating sub containers to create hierarchies that are six levels deep for better management of resources.		
21	Compute/VM should support decoupled server virtualization from the hypervisor and encapsulated it in its own hardware/software layer, this architecture results in lower overall risk for tenants of cloud infrastructure		
22	cloud infrastructure should support hardware root of trust to reduce the risk of firmware-level attacks against cloud tenants		
23	Monitors tenancies and determines if resources are in a state of weakened security, or if resources under attack. Machine Learning based technology automatically takes corrective action where possible		
24	Analyzes infrastructure operations in real-time and blocks operations that weaken a customer’s security		
25	Cloud service should provide a mechanism to test the effects of access control policies that are attached to users, groups, and roles before committing the policies into production		
26	Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections		

Database

S.No	Description	Compliance (Yes/No)	Reference
1	CSP should support as managed services for oracle database enterprise edition.		

S.No	Description	Compliance (Yes/No)	Reference
2	CSP should provide VMs and dedicated bare metal server option to run database		
3	CSP should able to provide complete automation for database lifecycle management e.g Provisioning de-provisioning, patching, backups, DR configuration, HA		
4	CSP should provide root access to OS on which DB system is hosted		
5	CSP should have capability of configuring, scheduling, performing and managing back-ups and restore activities (when required) ofall the data including but not limited to files, folders, images, system state, databases and enterprise applications in an encrypted manner		
6	CSP should have another Data Centre to host Disaster Site (DR) in same country but in different seismic zone		
7	There should be option of configuring Disaster Recovery environment in SYNC and ASYNC mode.		
8	The same Database should support mixed OLTP/OLAP workloads		
9	RDBMS should have native clustering with objectives of scalability and high availability. The solution should provide single image database concurrently accessed by multiple database servers		
10	RDBMS should have capabilities of running cluster with active-active configuration. Both nodes in a cluster should be active and participate in load balanced manner to handle load and provide maximum performance.		
11	RDBMS should provide database aware strong encryption capabilities within database for stored information in the tables as well as the information transmitted over network.		
12	Database should support option of different partitioning schemes within the database to split large volumes of data into separate pieces or partitions, which can be managed independently. It should support physical columns. The partitioning should enhance the performance, manage huge volumes of data and should provide foundation for Information Life Cycle Management.		
13	Must provide support to In-memory database transactions, able to process both row and column based data format in-memory simultaneously		
14	The database should able to repair specific corrupt blocks from far DR, without getting into recovery process form backup.		
15	Database instance scaling up & down with no downtime means no impact to business application during scaling operation		

S.No	Description	Compliance (Yes/No)	Reference
16	Data encryption both at database & storage level (at rest & motion)		
17	Cloud service should support copying snapshots of any size between different cloud provider regions for disaster recovery purposes		
18	Cloud service should support creating a DB snapshot and restoring a DB instance from a snapshot		
19	Data security to ensure Configuration drift assessment, User wise risk assessment, overall activity audit reporting, in data set find out sensitive data discovery		
20	Should provide database management tooling like cloning, backups & management & monitoring SQL performance		
21	Proposed Service Should be in Gartner Data management solutions		

Cloud Posture Management Solution

S. No	Description	Compliance (yes/no)	Reference
1	A cloud native solution that provides detect-and-respond framework. It must a) examine the cloud resources for weakness related to configuration and these problems shall be mapped to Center for Internet Security (CIS) Benchmarks. b) examine the cloud resources for weakness related to the operators and users for risky activities. c) detect patterns of activity that indicate possible malicious attempts to gain access to resources in the cloud environment and use them for corrupt purposes.		
2	It shall provide a single view into the overall cloud security posture. The dashboard should incorporate a number of different analytics that help security personnel identify, triage, and prioritize different cloud security issues.		
3	The solution shall incorporate the use of a cloud security scorecard, so that administrators have a quantitative measure to manage risk over time.		
4	Security analysts can drill down into a problem and leverage the problem details such as the resource name, resource type, compartment, detection time,		

S. No	Description	Compliance (yes/no)	Reference
	etc. to further investigate.		
5	The solution must provide recommendations page to quickly locate and resolve the highest priority problems that have been detected.		
6	Every problem identified shall be automatically assigned a severity and can be grouped by compartment, region, or resource type within the dashboard. Upon detection, the solution shall suggest, assist, or take corrective actions, based on your configuration.		
7	Sensitive information on the problems page, in the problem details and history shall be masked and viewable only by authorized users.		
8	Shall include built-in detection rules that defines resources to be monitored, with specific actions or configurations to trigger a problem reporting. It shall have rule-based conditions based on time, system version, user, tag, IP address metadata, and resource identifier.		
9	The solution shall provide flexibility to take action on security issues either manually or automatically.		
10	Shall include built-in rules on actions to be taken to resolve a problem.		
11	Flexibility to create new rules, enable/disable the rule, change the rule setting and risk levels		
12	Ability to create, modify and delete a reusable list of parameters which can set the scope for detection and responding rules. This list shall include not limited to : a) Trusted IP address : exempt listed IP address from triggering alerts b) resources that should be public : exempt listed resources from detection c) Groups of users with specific authorization : exempt listed groups or user from triggering alerts on activities users are authorized to perform		
13	Ability to view, sort and filter the list of problems		
14	Ability to send notification via email and slack for selected problems you want to notified.		
15	Shall provide data masking capability to specify categories of sensitive problem information to be redacted for a particular IAM user group or targets		
Threat Detector (TD)			
16	threat detector shall be aligned with MITRE attack framework		
17	Shall analyze real-time and historical events together with data from Threat Intelligence Service to produce correlated, high-fidelity security alerts		

S. No	Description	Compliance (yes/no)	Reference
18	Shall integrate with threat intelligence services to provide contextual information about the threat indicators found in the environment		
19	Critical events shall be prioritized and surfaced as problems for immediate response		
20	Shall provide full understanding of resources that are compromised		
21	It shall be proactive in monitoring budding incidents as they develop		
22	It shall provide comprehensive view of chain of events that drive scoring		
23	It should support model training, with global inference and tenant-level feedback. Models shall be tuned to detect malicious activities across long periods of time and report back details like Severity and Confidence levels, impacted resources and IP address help create a clear picture.		
24	It shall have the ability to detect attacks like password spraying, which can span multiple tenancies and regions.		
25	It shall support intent-based correlation and scoring Alerts that combine sightings of different behaviors scored according attack progression surface the right information without distractions.		

Cloud Audit service

S. No	Description	Compliance (yes/no)	Reference
1	The Cloud Infrastructure Audit service automatically records calls to all supported Cloud Infrastructure public application programming interface (API) endpoints as log events. Currently, all services support logging by Audit. Object Storage service supports logging for bucket-related events, but not for object-related events.		
2	Log events recorded by the Audit service include API calls made by the Cloud Infrastructure Console, Command Line Interface (CLI), Software Development Kits (SDK), your own custom clients, or other Cloud Infrastructure services.		
3	Information in the logs includes the following: Time the API activity occurred, Source of the activity, Target of the activity, Type of action, Type of response		

S. No	Description	Compliance (yes/no)	Reference
4	Each log event includes a header ID, target resources, timestamp of the recorded event, request parameters, and response parameters. You can view events logged by the Audit service by using the Console, API, or the SDK for Java. Data from events can be used to perform diagnostics, track resource usage, monitor compliance, and collect security-related events.		
5	Viewing Audit Log Events: When viewing events logged by Audit, you might be interested in specific activities that happened in the tenancy or compartment and who was responsible for the activity. You will need to know that the approximate time and date something happened and the compartment in which it happened to display a list of log events that includes the activity in question. List log events by specifying a time range on the 24-hour clock in Greenwich Mean Time (GMT), calculating the offset for your local time zone, as appropriate. New activity is appended to the existing list, usually within 15 minutes of the API call, though processing time can vary.		
6	Searching and Filtering in the Console: When you navigate to Audit in the Console, a list of results is generated for the current compartment. Audit logs are organized by compartment, so if you are looking for a particular event, you must know which compartment the event occurred in. You can filter the list in all the following ways: Date and time, Request Action Types(operations), Keywords		
7	Bulk Export of Audit Log Events:		
8	You can request a bulk export of audit logs, and within 5-10 business days cloud support will begin making copies of the logs and adding them to buckets in your tenancy.		
9	The export includes logs for the specified regions, beginning after you make the request and continuing into the future.		
10	Administrators have full control of the buckets and can provide access to others with IAM policy statements.		
11	Exported logs remain available indefinitely.		
12	Specify all the regions you want exported in your request. If you only request some regions, then decide later you want to add other regions, you must make another request.		

Cloud WAF Service

S.No.	Description	Compliance (yes/no)	Reference
1	Shall be an enterprise-grade, cloud-based web application firewall that can be attached to an enforcement point such as load balancer or web application domain name protecting against malicious and unwanted internet traffic.		
2	The ability to create and manage rules for internet threats including and not limited to : 1) Malicious bots 2) Application layer (L7) DDOS attacks 3) SQL injections 4) cross-site scripting 5) vulnerabilities defined by OWASP 6) access rules to limit based on geography, IP address, URL or signature of the request		
3	Ability to define explicit actions for requests that meet various conditions. Actions include : 1) to log and allow 2) detect 3) block 4) redirect 5) bypass 6) show a CAPTCHA for all matched requests		
4	Access rules shall support the following conditions: 1) URL 2) IP address 3) country/region 4) user agent 5) HTTP header 6) HTTP method Action to be performed when request rules are met shall be configurable. It should have a default action when requests dont match any of the rules defined		
5	Shall provide predefined WAF protection rules and rulesets for OWASP top ten. These rules shall be kept up to date with CRS and CVEs.		

S.No.	Description	Compliance (yes/no)	Reference
6	Shall mitigate undesired bot traffic from the site using any of the following detection tools. 1) Javascript challenge 2) Human Interaction Challenge 3) Device Fingerprint Challenge 4) Captcha		
7	Shall include a list of good bots managed by known providers, such as Baidu or Google. Ability to allow the access from a specific good bot, or block the bot if they serve no business purpose.		
8	Ability to customize the comments for the CAPTCHA Challenge for each URL.		
9	After the WAF policies have been created, the solution shall detect and provide recommendations rules that produce the least number of false positives and still provide good protection.		
10	The ability to define and apply custom protection rules from open source firewall modules to your WAF configurations, such as Mod Security modules.		
11	Provides caching rules to selectively cache requested file.		
12	Shall integrate with 3rd party threat intelligence sources and known IP address shall be updated on a daily basis.		
13	WAF logs shall be retender as per corporate retention policy		
14	Shall provide rate limiting rules to limit the frequency of requests for each unique client IP address		
15	Ability to add firewall to a WAF policy, update and delete and moving to another compartment		
16	Ability to view the firewalls associated with a specified WAF policy or get details of a specific firewall.		
17	Shall provide action management i.e ability to add actions to WAF policies to determine whether the response to a request is allowed, allowed but logged, or returns a specified HTTP response. These actions can be reused between different WAF policies		
18	Shall provide the ability to manage network address list , including creation, updating and deletion		

Vulnerability Scanning Service

S.No	Description	Compliance (yes/no)	Reference
1	The Scanning service shall identify the following security issues in the compute instances : (a) Ports that are unintentionally left open might be a potential attack vector to your cloud resources, or enable hackers to exploit other vulnerabilities. (b) OS packages that require updates and patches to address vulnerabilities (c) OS configurations that hackers might exploit (d) compliance with the section 5 (Access, Authentication, and Authorization) benchmarks defined for Distribution Independent Linux.		
2	Ability to scan individual or all compute instances within a compartment and its sub compartments.		
3	It shall detect vulnerabilities using the following vulnerability sources : (a) Using Industry-standard benchmarks published by the Center for Internet Security (CIS). (b) Using National Vulnerability Database (c) Using Open Vulnerability and Assessment Language (OVAL)		
4	The Scanning service shall detect vulnerabilities in the following platforms: a) Oracle Linux b) CentOS c) Ubuntu d) Windows		
5	It shall provide the following information for every vulnerability detected a) CVE ID b) Risk Level c) CVE description d) last detected e) first detected.		
6	Shall provide the following details for each CIS benchmark that the scanning service tested on the compute instance : 1) Benchmark ID 2) Result : Pass / Fail 3) Summary		
7	Shall support the following port scanning : 1) Network mapper searches your public IP address for open ports 2) leverage on agent to check of open ports that are not accessible from		

S.No	Description	Compliance (yes/no)	Reference
	public address		
8	Host Vulnerabilities Reports: Vulnerability Scanning Service scans your targets based on the schedule and scanning properties in the recipe assigned to each target. Use vulnerabilities reports to identify security issues in your compute instances like critical OS patches.		
9	The scanning service shall scan images in Cloud Infrastructure Registry for potential security vulnerabilities.		
10	The vulnerability scanning service shall integrate with Cloud Guard. Shall use Cloud Guard to detect and respond to security vulnerabilities identified by Vulnerability Scanning Service.		
11	Ability to schedule the scanning service		
12	Vulnerability report can be exported as a CSV format for offline analysis		

Threat Intelligence

S. No	Description	Compliance (yes/no)	Reference
1	Shall provide access to built-in threat Intelligence including and not limited to : a) indicators of compromise b) threat reputation data c) geolocation data d) known bad actors e) confidence levels		
2	Shall automatically aggregate and curate insights from elite security researchers based on industry-standard open source feeds and third-party partners.		
3	Support out-of-the-box integration with SOC and provide actionable guidance for threat detection and prevention		
4	Shall provide contextual information about the threat indicators found in the environment		
5	Threat indicator shall take into consideration the previous observations or behavior and this shall include related tactics, techniques, and procedures.		
6	Shall provide an overall Confidence Score on the likelihood that the indicator is associated with malicious behavior.		

Other

S. No	Description	Compliance (yes/no)	Reference
1	In Case, any dispute happens between DTAP & MSP during the execution of the project (contract period), the CSP must ensure the hosted application and related services remain live in the cloud environment without any disruption.		

All these compliances are required to be submitted on CSP letter head. The Public URL may be provided in a separate file in clickable format. Non-compliant bids will be rejected without any further queries.

Note related to Technical Qualification Evaluation

a. The Bidders are required to submit all required documentation in support of the evaluation criteria specified (e.g. detailed project citations and completion certificates, and all others) as required for technical compliance.BEC may ask Bidder(s) for additional information/clarifications to verify claims made in Technical Bid documentation from the Bidder on the already submitted Technical Proposal at any point of time before opening of the commercial bid. The primary function of additional information/clarifications in the evaluation process is to clarify ambiguities and uncertainties arising out of the evaluation of the bid documents. Oral / written clarifications provide the opportunity for the BEC / DTAP to seek required clarifications and for the bidder to provide the same. DTAP and the committee may seek inputs from their professional, technical experts in the evaluation process. However, the bidder will not be allowed to modify or amend their proposals during these clarifications.

14.3 Form-TQ3: Unpriced Bill of Material (BOM) for the Solution

14.3.1 Capex

14.3.1.1 Additional Software License

Sl #	Component	Description	Quantity	Unit of Measure	Data sheet Reference

14.3.2 Opex

14.3.2.1 Hosting Infrastructure

Sl #	Component	Description	Quantity	Unit of Measure	Data sheet Reference

14.4 Form-TQ4: Manufacturer's Authorization Form (MAF)/ CSP Authorization Form.

[2 separate forms has to be provided by the MSP each for the Database Licenses & Cloud Services proposed in the name of below mentioned details as per standard format from OEM]

Date:
To,
THE DIRECTOR,
TREASURY, ACCOUNTS & PENSION,
INDRAWATI BHAWAN, BLOCK 1
1st FLOOR, NAWA RAIPUR,
ATAL NAGAR CHHATTISGARH

NOTE:

- The letter should be submitted on the letter head of the CSP and should be signed by the authorized signatory.

15. ANNEXURE III: COMMERCIAL BID TEMPLATES

[Cover Letter 4]

15.1 Form-CP1: Commercial Bid Covering Letter

[To be submitted by the lead bidder on its letterhead]

Date: DD/MM/YYYY

To,

The Director, Directorate of Treasury, Account & Pension,
Government of Chhattisgarh,
1st Floor, A Block, Indravati Bhawan,
Nawa Raipur Atal Nagar, Chhattisgarh – 492101

Subject: Submission of the commercial bid for selection of MSP/CSP for hosting, commissioning, data migration and O&M of e-Kosh application on cloud environment

Dear Sir,

We, the undersigned, offer to provide services for hosting, commissioning, data migration and O&M of e-Kosh application on cloud environment project with reference to your Request for Proposal bearing < RFP reference number> dated < date> and our technical proposal. Our Commercial Bid is provided in the form below. The amount is inclusive of all duties, taxes and levies including GST.

- **PRICE AND VALIDITY**
  - The price quoted in our bid is in accordance with the terms as specified in the RFP documents. The price and other terms & conditions of this Bid are valid as per the bid validity specified in the final RFP document,
  - We hereby confirm that our prices include all taxes and cess (if any) including income tax and professional tax including GST,
  - We understand that the actual payment would be made as per the prevailing GST rates during the time of payment.
- **UNIT RATES**
  - We have indicated in the relevant forms the unit rates
- **BID PRICING**
  - We further confirm that the prices stated in our bid are in accordance with your Instruction to Bidders included in RFP documents.
- **BID PRICE**
  - We declare that our bid prices are for the entire scope of the work as specified in the Requirements specified in the bid documents.
- **QUALIFYING DATA**

- We confirm having submitted the information as required by you in your Instruction to Bidders. In case you require any other further information / documentary proof in this regard before evaluation of our bid, we agree to furnish the same in time to your satisfaction.

- **PERFORMANCE BANK GUARANTEE**
  - We hereby declare that in case the contract is awarded to us, we shall submit the Performance Bank Guarantee as specified in this RFP document (Refer Bid fact Sheet).
  - Our Commercial Bid shall be binding upon us subject up to expiration of the validity period of the Proposal. We understand you are not bound to accept any Proposal you receive. We agree to abide by all the terms and conditions of this RFP document. We hereby declare that our bid is made in good faith, without collusion or fraud and the information contained in the bid is true and correct to the best of our knowledge and belief.

Yours sincerely,

(Authorized Signatory)
(Name, Designation, Address, Contact Details, Seal, Date) Form-CP2: Commercial Proposal Forms

15.2 Form-CP2: Commercial Proposal Forms

15.2.1 Summary of Costs

S. No.	Cost Item	Amount (INR) (inclusive of all taxes)
A=A1+A2	**Hosting, Commissioning, data migration of e-Kosh Application**	
A1	Capex Cost	
A2	Opex Cost	
Total Bid Value (TBV) = A		
Total Bid Value (in words)		

Note:

i. All quoted prices should be inclusive of all taxes and duties prevailing on the date of proposal submission.
ii. Prices are valid for a period of 365 Days from date of submission of Bid.
iii. The bidder is expected to account for all services/ hosting/commissioning/data migration/support required to make the implementation successful as part of total contract value.
iv. DTAP reserve the right to increase or decrease the no. of resources / other items quantity at the time of Agreement or during the project.
v. Price Bid evaluation shall be done on the basis of Total Bid Value (TBV) captured in the above table
vi. **All forms/ sub forms from 15.2.1 to 15.2.4 are required to be signed, sealed and uploaded as part of financial submission**. In case there is a difference between online portal submission vs scan copy the scan copy shall take precedence for form 15.2.1.
vii. In case other forms uploaded are not consistent with summary specified in 15.2.1, bid evaluation shall be done as per form 15.2.1. While making payments lower of the two values shall be referred.

15.2.2 Form A1: Capex Cost

The component specific cost is described below:

S. No.	Item	Form	Total Cost (including taxes)
1	**Additional Software License Cost**	Form A1-a	
2	**Initial Set up Cost for Cloud Environment**	Form A1-b	
3	**Hosting of existing application and data migration of existing system in Cloud environment**	Form A1-c	
4	**Any additional Capex Cost (Please add separate line item if any)**		
	Total Capex Cost		

Note:

- The bidder should take due care that the costs mentioned in summary sheet should match the cost mentioned in detailed sheet (forms). However, in case of any discrepancies, the cost mentioned in the detailed sheets will prevail.
- Section 15.2.2 must be mandatorily uploaded in the price bid section (Envelope C) at appropriate place holders defined as pdf Format.

15.2.2.1 Form-A1-a: Additional Software License Cost

S. No.	Paticulars			Capex Cost				Total Cost [Σd]
	Software Component	Make, Model & Version	Quantity [a]	Unit of Measurement (Per Core/ Per Users/ etc.)	Unit Price (exclusive of any taxes) [b]	Tax (Per Unit) [c]	Capex Amount (inclusive of all taxes) [d= a x (b+c)]	
1.	Oracle Database EE Edition		12					
2.	Partitioning		12					
3.	Oracle Tuning Pack		12					
4.	Oracle Diagnostic Pack		12					

Note:

- The bidder is required to fill the above format with each component. In case, one component requires more than one software then separate line items should be created as required.
- In case the cost is found to be missing for any component, then it will be assumed that there is no cost for the concerned component.

15.2.2.2 Form-A1-b: Initial Set up of the Cloud environment

S. No.	Particulars	Capex Cost (a)	Applicable Taxes (b)	Total Cost in INR (inclusive of Taxes) (c=a+b)
1.	Cost for Initial Set up of the Cloud Environment			

Note:

- The bidder is required to fill the above format with each component.
- In case the cost is found to be missing for any component, then it will be assumed that there is no cost for the concerned component.

15.2.2.3 Form-A1-c: Hosting of Application &Migration of existing system in Cloud environment

S. No.	Particulars	Capex Cost (a)	Applicable Taxes (b)	Total Cost in INR (inclusive of Taxes) (c=a+b)	Total Cost [Σ c]
1.	Hosting of Application Cost				
2.	Data Migration Cost				

Note:

- The bidder is required to fill the above format with each component.
- In case the cost is found to be missing for any component, then it will be assumed that there is no cost for the concerned component.

15.2.3 Form A2: Opex Cost

15.2.3.1 Form A2: Cloud Hosting Cost

S. No.	Item	Form	Total Cost (including taxes)
1	**Price for Cloud Services (at Data Center)**	Form A2-a	
2	**Price for Cloud Services (at Disaster Recovery)**	Form A2-b	
3	**Manpower Deployment**	Form A2-c	
	Total Opex Cost		

Note:

- For the cloud hosting charges, MSP shall quote an estimated charge as mentioned above for 36 months. The payments from DTAP shall be made on actual basis as per the invoice of the Cloud Service Provider but capped at the estimated charge quoted for 1 month by the bidder for such cloud/ hosting charges as well as managed services. No cost escalation will be accepted by DTAP in this regard during the duration of the contract. The bidder is expected to consider industry best practices to optimize the hosting charges thus reducing DTAP total cost of ownership.
- In the above table, MSP is required to quote estimated total cost for 36 months inclusive of all kinds of applicable taxes for the entire period of Operations & Maintenance (O&M) phase.

15.2.3.2 Form-A2-a: Price for Cloud Services (at Data Center)

Following is the requirement for hardware's at **Data Center**. Kindly quote the price against each of the component for 1 month.

Cloud Service	Metric	Unit Price (a)	Taxes (b)	Price with Tax (c = a + b)	Quantity (d)	Total Price (Including Taxes) (e= c x d)
Oracle Database Cloud Service – (CSP Native Managed Service)	vCPU/Hour				64	
Compute – CPU	vCPU/Hour				88	
Compute – Memory	GB/Hour				352	
Block Storage (Boot Volume for Servers)	Gigabyte Storage Capacity/Month				5120	
Block Storage (Storage for data)	Gigabyte Storage Capacity/ Month				5120	
Storage IOPS (50 IOPS/GB)	Performance Units/Gigabyte/ Month				51200	
Database backup Service	Gigabyte Storage Capacity/Month				5120	
Backup Storage (Object Storage)	Gigabyte Storage Capacity/Month				5120	
Load Balancer Base	LB Hour				2	
Load Balancer Bandwidth	Mbps/Hour				400	
DNS Service	1M Queries				1	

Cloud Service	Metric	Unit Price (a)	Taxes (b)	Price with Tax (c = a + b)	Quantity (d)	Total Price (Including Taxes) (e= c x d)
DNS Traffic Management	1M DNS Traffic Management Queries				1	
Next Generation Network Firewall Service with IPS in HA	Instance/Hour				1	
Web Application Firewall – Requests	1M Incoming Requests/Month				10	
Web Application Firewall – Instance	Instance/Month				2	
OS Management Service	Instance/Month				20	
Cloud Audit Service	Instance/Month				20	
Cloud Security Posture Management Solution	Instance/Month				20	
Public IP	Instance/Month				20	
Threat Intelligence	Instance/Month				20	
Vulnerability Scanning Service	Instance/Month				20	
Antivirus	Instance/Month				10	
Outbound Traffic	GB/Month				10240	
Any other component (additional line and details to be added accordingly)						
Total Cost for 1 month (in words) [Σe] = f						
Total cost for 36 months [f x 36]						

15.2.3.3 Form-A2-b: Price for Cloud Services (at Disaster Recovery)

Following is the requirement for hardware's at **Disaster Recovery.** Kindly quote the price against each of the component for 1 month.

Cloud Service	Metric	Unit Price (a)	Tax (b)	Unit Price with Tax (c = a + b)	Quantity (d)	Total Price (Including Taxes) (e= c x d)
Oracle Database Cloud Service – (CSP native Managed Service)	vCPU/Hour				16	
Compute – CPU	vCPU/Hour				22	
Compute – Memory	GB/Hour				88	
Block Storage (Boot Volume for Servers)	Gigabyte Storage Capacity/Month				5120	
Block Storage (Storage for data)	Gigabyte Storage Capacity/ Month				5120	
Storage IOPS (60 IOPS/GB)	Performance Units/Gigabyte/ Month				51200	
Load Balancer Base	LB Hour				2	
Load Balancer Bandwidth	Mbps/Hour				400	
DNS Service	1M Queries				1	
DNS Traffic Management	1M DNS Traffic Management Queries				1	
Next Gen Network Firewall Service with IPS in HA	Instance/Hour				1	
Web Application Firewall – Requests	1M Incoming Requests/Month				10	
Web Application Firewall – Instance	Instance/Month				2	
OS Management Service	Instance/Month				20	
Cloud Audit Service	Instance/Month				20	
Cloud Security Posture Management Solution	Instance/Month				20	

Cloud Service	Metric	Unit Price (a)	Tax (b)	Unit Price with Tax (c = a + b)	Quantity (d)	Total Price (Including Taxes) (e= c x d)
Public IP	Instance/Month				20	
Threat Intelligence	Instance/Month				20	
Vulnerability Scanning Service	Instance/Month				20	
Antivirus	Instance/Month				10	
Any other component (additional line and details to be added accordingly)						
Total Cost for 1 month (in words) [Σe] = f						
Total cost for 36 months [f x 36]						

15.2.4 Form A2-C: Person-Month charges for resources required to be deployed onsite

S. No.	Position	Per Person Month Cost in INR (b)	Applicable Taxes (c)	Per Person Month Cost in INR (inclusive of taxes) (d = b + c)	Total Cost [Σ d]	Total Cost 36 months [Σ d x 36]
1.	Cloud Support Engineer					

Note: The rate quoted above shall be utilized for any applicable deductions due to non-availability of the resources onsite.

16. ANNEXURE IV: OTHER TEMPLATES

16.1 Format For Performance Bank Guarantee

[The Performance Guarantee should be issued by the nationalized/scheduled bank having an operational branch in the State of Chhattisgarh.]

Date: ____________

Bank Guarantee No.: __________________

To,

The Director, Directorate of Treasury, Account & Pension,
Government of Chhattisgarh,
1st Floor, A Block, Indravati Bhawan,
Nawa Raipur Atal Nagar, Chhattisgarh – 492101

WHEREAS ___________________ (name of firm (hereinafter called 'MSP') has undertaken, in pursuance the RFP No.__________ , Dated ______ of Director, Directorate of TREASURY, ACCOUNTS & PENSION, FD (GoCG) (hereinafter called the 'DTAP') to provide services for Hosting, Commissioning, data Migration and O&M of e-Kosh application on cloud environment AND WHEREAS in terms of the tender conditions the MSP is required to furnish to the DTAP a Bank Guarantee for a sum of ₹ _____________ (Rupees ___________________) as Performance Bank Guarantee against the MSP's offer aforesaid.

AND WHEREAS we, ___________________ Bank, ___________________ branch, have at the request of the MSP agreed to give to the DTAP this guarantee as hereinafter contained.

And whereas we, a banking company incorporated and having its head/registered office at <Address> and having one of its office at <Address> have agreed to give the supplier such a bank guarantee.

Now, therefore, we hereby affirm that we are guarantors and responsible to you, on behalf of the bidder, up to a total of ₹ <Insert amount> and we undertake to pay you, upon your first written demand declaring the supplier to be in default under the contract and without cavil or argument, any sum or sums within the limits of ₹ <Insert amount> as aforesaid, without your needing to prove or to show grounds or reasons for your demand or the sum specified therein.

We hereby waive the necessity of your demanding the said debt from the Bidder before presenting us with the demand. We further agree that no change or addition to or other modification of the terms of the contract to be performed there under or of any of the contract documents which may be made between you and the Bidder shall in any way release us from any liability under this guarantee and we hereby waive notice of any such change, addition or modification. This Guarantee shall be valid until <Insert Time>

Notwithstanding anything contained herein:

1. Our liability under this bank guarantee shall not exceed ₹ <Insert amount>
2. This bank guarantee shall be valid up to <insert period>
3. It is condition of our liability for payment of the guaranteed amount or any part thereof arising under this bank guarantee that we receive a valid written claim or demand for payment under this bank guarantee on or before <insert time period> failing which our liability under the guarantee will automatically cease.

(Authorized Signatory of the Bank)

(Name, Designation, Address, Seal, Date)

17. *MASTER SERVICE AGREEMENT*

THIS MASTER SERVICE AGREEMENT ("Agreement") is made on this the <***> day of <***> 20… at <***>, India.

BETWEEN

-- having its office at --- India hereinafter referred to as 'Purchaser' / 'Purchaser' or '----------------', which expression shall, unless the context otherwise requires, include its permitted successors and assigns);

AND

<***>, a Company incorporated under the Companies Act, 1956, having its registered office at <***> (hereinafter referred to as 'the Managed Service Provider' which expression shall, unless the context otherwise requires, include its permitted successors and assigns).

Each of the parties mentioned above are collectively referred to as the 'Parties' and individually as a 'Party'.

WHEREAS:

1. Purchaser is desirous to procure the Cloud services.
2. In furtherance of the same, Purchaser undertook the selection of a suitable Managed Service Provider through a competitive bidding for implementing the Project and in this behalf invited bids dated <***>.
3. The successful bidder has been selected as the Managed Service Provider on the basis of the bid response to undertake the execution of the Project.

NOW THEREFORE, in consideration of the mutual covenants, promises, assurances, representations and provisions set forth herein, the Parties hereto agree as follows:

17.1 Definitions and Interpretations

17.1.1 Definitions

Terms and expressions used in this Agreement shall have the meanings set out below.

Term	Meaning
Adverse Effect	means material adverse effect on (a) the ability of the Managed Service Provider to exercise any of its rights or perform/discharge any of its duties/obligations under and in accordance with the provisions of this Agreement and/or (b) the legal validity, binding nature or enforceability of this Agreement;
Agreement	means Master Services Agreement along with Service Level Agreement and Non-Disclosure Agreement
Applicable Law(s)	means any statute, law, ordinance, notification, rule, regulation, judgment, order, decree, bye-law, approval, directive, guideline, policy, requirement or other governmental restriction or any similar form of decision applicable to the relevant party and as may be in effect on the date of the execution of this Agreement and during the subsistence thereof, applicable to the Project;
Confidential Information	means all information including Purchaser Data (whether in written, oral, electronic or other format) which relates to the technical, financial and business affairs, dealers, suppliers, products, developments, operations, processes, data, trade secrets, design rights, know-how, plans, budgets and personnel of each Party and its affiliates which is disclosed to or otherwise learned by the other Party in the course of or in connection with this Agreement (including without limitation such information received during negotiations, location visits and meetings in connection with this Agreement); All such information in whatever form or mode of transmission, which is disclosed by a Party (the "Disclosing Party") to any other Party (the "Recipient") in connection with the Project during its implementation and which has been explicitly marked as "confidential", or when disclosed orally, has been identified as confidential at the time of disclosure and has been confirmed and designated in writing within <15 days> from oral disclosure at the latest as confidential information by the Disclosing Party, is "Confidential Information".

Control	means, in relation to any business entity, the power of a person to secure by means of the holding of shares or the possession of voting power in or in relation to that or any other business entity, or by virtue of any powers conferred by the articles of association or other document regulating that or any other business entity, that the affairs of the first mentioned business entity are conducted in accordance with that person's wishes and in relation to a partnership, means the right to a share of more than one half of the assets, or of more than one half of the income, of the partnership;
Deliverables	means the services, products, solution and infrastructure agreed to be delivered by the Managed Service Provider in pursuance of the Agreement as defined more elaborately in the scope of work and includes all documents related to the user manual, technical manual,
	design, process and operating manuals, service mechanisms, policies and guidelines (such as security related, data migration related), inter alia payment and/or process related etc., source code and all its modifications;
GoI	means the Government of India;
Intellectual Property Rights	means all rights in written designs and copyrights, moral rights, rights in databases and Bespoke Software / Pre-existing work including its up-gradation systems and compilation rights (whether or not any of these are registered and including application for registration);
Material Breach	means a breach by either Party (Purchaser or Managed Service Provider) of any of its obligations under this Agreement which has or is likely to have an Adverse Effect on the Project which such Party shall have failed to cure;
Parties	means Purchaser and Managed Service Provider for the purposes of this Agreement and "Party" shall be interpreted accordingly;
Purchaser Data	means all proprietary data of the Government Department or its nominated agencies generated out of operations and transactions, documents all taxpayers data and related information including but not restricted to user data which the Managed Provider obtains, possesses or processes in the context of providing the Services to the users pursuant to this Agreement;
Services	means the services delivered to the Stakeholders of Purchaser or its nominated agencies, employees of Purchaser or its nominated agencies, and to professionals, using the tangible and intangible assets created, procured, installed, managed and operated by the Managed Service Provider including the tools of information and communications technology

Service Level	means the level of service and other performance criteria which will apply to the Services delivered by the Managed Service Provider;
SLA	means the Availability, Performance, Security, Support, Helpdesk, Disaster Recovery, Audit, Monitoring and other SLAs executed as part of this Master Service Agreement;
Stakeholders	means Purchaser or its nominated agencies, citizens, employees, Departments of State Government, etc.

17.1.2 Interpretation

In this Agreement, unless otherwise specified:

a) references to Clauses, Sub-Clauses, Paragraphs, Schedules and Annexures are to clauses, sub-clauses, paragraphs, schedules and annexures to this Agreement;

b) use of any gender includes the other genders;

c) references to a ‘company’ shall be construed so as to include any company, corporation or other body corporate, wherever and however incorporated or established;

d) references to a ‘person’ shall be construed so as to include any individual, firm, company, government, state or agency of a state, local or municipal authority or government body or any joint venture, association or partnership (whether or not having separate legal personality);

e) a reference to any statute or statutory provision shall be construed as a reference to the same as it may have been, or may from time to time be, amended, modified or reenacted;

f) references to times are to Indian Standard Time;

g) a reference to any other document referred to in this Agreement is a reference to that other document as amended, varied, novated or supplemented at any time; and

h) all headings and titles are inserted for convenience only. They are to be ignored in the interpretation of this Agreement.

17.1.3 Measurements and Arithmetic Conventions

All measurements and calculations shall be in the metric system and calculations done to two decimal places, with the third digit of five or above being rounded up and below five being rounded down except in money calculations where such amounts shall be rounded off to the nearest INR.

17.1.4 Ambiguities within Agreement

In case of ambiguities or discrepancies within this Agreement, the following principles shall apply:

a) as between two Clauses of this Agreement, the provisions of a specific Clause relevant to the issue under consideration shall prevail over those in a general Clause;

b) as between the provisions of this Agreement and the Schedules/Annexures, the Agreement shall prevail, save and except as expressly provided otherwise in the
Agreement or the Schedules/Annexures; and

c) as between any value written in numerals and that in words, the value in words shall prevail.

17.2 Term and Duration of the Engagement

This Agreement shall come into effect on <***> 201- (hereinafter the 'Effective Date') and shall continue till operation and maintenance completion date which shall be the date of the completion of the operation and maintenance to the Purchaser or its nominated agencies, unless terminated earlier (as per Clause 1.13), in which case the contract will get terminated on fulfillment of all obligations mentioned as per Clause 1.13 and 1.23.

17.3 Conditions Precedent

17.3.1 Provisions to take effect upon fulfillment of Conditions Precedent

Subject to express terms to the contrary, the rights and obligations under this Agreement shall take effect only upon fulfillment of all the Conditions Precedent set out below. However, Purchaser or its nominated agencies may at any time at its sole discretion waive fully or partially any of the Conditions Precedent for the Managed Service Provider.

For the avoidance of doubt, it is expressly clarified that the obligations of the Parties (or its nominated agencies) under this Agreement shall commence from the fulfillment of the Conditions Precedent as set forth below.

17.3.2 Conditions Precedent of the Managed Service Provider

The Managed Service Provider shall be required to fulfill the Conditions Precedent which is as follows:

a) to provide a Performance Security/Guarantee, if demanded by the Purchaser, and other guarantees/ payments within <21 days> of the receipt of notification of award from the
Purchaser; and

b) to provide the Purchaser or its nominated agencies certified true copies of its constitutional documents and board resolutions authorizing the execution, delivery and performance of this Agreement by the Managed Service Provider (optional).

17.3.3 Conditions Precedent of the Purchaser

The Purchaser shall be required to fulfill the Conditions Precedents which are as follows:

a) Handing over of <project office> (if applicable)

b) Necessary clearances associated with the execution of the project, unless specified to be performed by the Managed Service Provider

c) Approval of the Project by a Competent Authority, etc.

17.3.4 Extension of time for fulfillment of Conditions Precedent

The Parties may, by mutual agreement extend the time for fulfilling the Conditions Precedent and the Term of this Agreement.

17.3.5 Non-fulfillment of the Managed Service Provider's Conditions Precedent

a) In the event that any of the Conditions Precedent of the Managed Service Provider has not been fulfilled within <15 days> of signing of this Agreement and the same have not been waived fully or partially by Purchaser or its nominated agencies, this
Agreement shall cease to exist;

b) In the event that the Agreement fails to come into effect on account of non-fulfillment of the Managed Service Provider's Conditions Precedent, the Purchaser or its nominated agencies shall not be liable in any manner whatsoever to the Service Provider and the Purchaser shall forthwith forfeit the Earnest Money Deposit, if taken.

c) In the event that possession of any of the Purchaser or its nominated agencies facilities has been delivered to the Managed Service Provider prior to the fulfillment of the Conditions Precedent, upon the termination of this Agreement such shall immediately revert to Purchaser or its nominated agencies, free and clear from any encumbrances or claims.

17.4 Change of Control

a) In the event of a change of control of the Managed Service Provider during the Term, the Managed Service Provider shall promptly notify Purchaser and/or its nominated agencies of the same.

b) In the event that the net worth of the surviving entity is less than that of Managed Service Provider prior to the change of control, the Purchaser or its nominated agencies may within 30 days of becoming aware of such change in control, require a replacement of existing Performance Guarantee, if applicable, furnished by the Managed Service Provider from a guarantor acceptable to the Purchaser or its nominated agencies (which shall not be Managed Service Provider or any of its associated entities).

c) If such a guarantee is not furnished within 30 days of the Purchaser or its nominated agencies requiring the replacement, the Purchaser may exercise its right to terminate this Agreement within a further 30 days by written notice, to become effective as specified in such notice.

d) Pursuant to termination, the effects of termination as set out in Clause 1.13 of this Agreement shall follow.

For the avoidance of doubt, it is expressly clarified that the internal reorganization of the Managed Service Provider shall not be deemed an event of a change of control for purposes of this Clause unless the surviving entity is of less net worth than the predecessor entity.

17.5 Representations and Warranties

17.5.1 Representations and warranties of the Managed Service Provider

The Managed Service Provider represents and warrants to the Purchaser or its nominated agencies that:

a) it is duly organized and validly existing under the laws of India, and has full power and authority to execute and perform its obligations under this Agreement and other agreements and to carry out the transactions contemplated hereby;

b) it is a competent provider of a variety of Cloud and managed services;

c) it has taken all necessary corporate and other actions under laws applicable to its business to authorize the execution and delivery of this Agreement and to validly exercise its rights and perform its obligations under this Agreement;

d) from the Effective Date, it will have the financial standing and capacity to undertake the Project in accordance with the terms of this Agreement;

e) in providing the Services, it shall use reasonable endeavors not to cause any unnecessary disruption to Purchaser's normal business operations;

f) this Agreement has been duly executed by it and constitutes a legal, valid and binding obligation, enforceable against it in accordance with the terms hereof, and its obligations under this Agreement shall be legally valid, binding and enforceable against it in accordance with the terms hereof;

g) the information furnished in the Managed Service Provider's response to the RFP and any subsequent clarification pertaining to the evaluation process, furnished on or before the date of this Agreement is to the best of its knowledge and belief true and accurate in all material respects as at the date of this Agreement;

h) the execution, delivery and performance of this Agreement shall not conflict with, result in the breach of, constitute a default by any of the terms of its Memorandum and Articles of Association or any Applicable Laws or any covenant, contract, agreement, arrangement, understanding, decree or order to which it is a party or by which it or any of its properties or assets is bound or affected;

i) there are no material actions, suits, proceedings, or investigations pending or, to its knowledge, threatened against it at law or in equity before any court or before any other judicial, quasi-judicial or other authority, the outcome of which may result in the breach of this Agreement or which individually or in the aggregate may result in any material impairment of its ability to perform any of its material obligations under this
Agreement;

j) it has no knowledge of any violation or default with respect to any order, writ, injunction or decree of any court or any legally binding order of any Government Instrumentality which may result in any Adverse Effect on its ability to perform its obligations under this Agreement and no fact or circumstance exists which may give rise to such proceedings that would adversely affect the performance of its obligations under this Agreement;

k) it has complied with Applicable Laws in all material respects and has not been subject to any fines, penalties, injunctive relief or any other civil or criminal liabilities which in the aggregate have or may have an Adverse Effect on its ability to perform its obligations under this Agreement;

l) no representation or warranty by it contained herein or in any other document furnished by it to Purchaser or its nominated agencies in relation to the Required Consents contains or shall contain any untrue or misleading statement of material fact or omits or shall omit to state a material fact necessary to make such representation or warranty not misleading; and

m) no sums, in cash or kind, have been paid or shall be paid, by it or on its behalf, to any person by way of fees, commission or otherwise for entering into this Agreement or for influencing or attempting to influence any officer or employee of Purchaser or its nominated agencies in connection therewith.

17.5.2 Representations and warranties of the Purchaser or its nominated agencies

Purchaser or its nominated agencies represent and warrant to the Managed Service Provider that:

a) it has full power and authority to execute, deliver and perform its obligations under this Agreement and to carry out the transactions contemplated herein and that it has taken all actions necessary to execute this Agreement, exercise its rights and perform its obligations, under this Agreement and carry out the transactions contemplated hereby; b) it has taken all necessary actions under Applicable Laws to authorize the execution, delivery and performance of this Agreement and to validly exercise its rights and perform its obligations under this Agreement;

c) it has the financial standing and capacity to perform its obligations under the Agreement;

d) it is subject to the laws of India, and hereby expressly and irrevocably waives any immunity in any jurisdiction in respect of this Agreement or matters arising thereunder including any obligation, liability or responsibility hereunder;

e) this Agreement has been duly executed by it and constitutes a legal, valid and binding obligation enforceable against it in accordance with the terms hereof and its obligations under this Agreement shall be legally valid, binding and enforceable against it in accordance with the terms thereof;

f) the execution, delivery and performance of this Agreement shall not conflict with, result in the breach of, constitute a default under, or accelerate performance required by any of the Applicable Laws or any covenant, contract, agreement, arrangement, understanding, decree or order to which it is a party or by which it or any of its properties or assets is bound or affected;

g) there are no actions, suits or proceedings pending or, to its knowledge, threatened against it at law or in equity before any court or before any other judicial, quasi-judicial or other authority, the outcome of which may result in the default or breach of this Agreement or which individually or in the aggregate may result in any material impairment of its ability to perform its material (including any payment) obligations under this Agreement;

h) it has no knowledge of any violation or default with respect to any order, writ, injunction or any decree of any court or any legally binding order of any Government Instrumentality which may result in any Adverse Effect on the Purchaser or its nominated agencies ability to perform its obligations under this Agreement and no fact or circumstance exists which may give rise to such proceedings that would adversely affect the performance of its obligations under this Agreement;

i) it has complied with Applicable Laws in all material respects;

j) all information provided by it in connection with the Project is, to the best of its knowledge and belief, true and accurate in all material respects; and

k) upon the Managed Service Provider performing the covenants herein, it shall not at any time during the term hereof, interfere with peaceful exercise of the rights and discharge of the obligations by the Managed Service Provider, in accordance with this Agreement.

17.6 Obligations of the Purchaser or its Nominated Agencies

Without prejudice to any other undertakings or obligations of the Purchaser or its nominated agencies under this Agreement, the Purchaser or its nominated agencies shall perform the following:

a) The key obligations and roles & responsibilities of the Purchaser is specified in thisRFP.

b) To provide any support through personnel to test the system/application/solution during the Term;

c) To provide any support through personnel and/or test data during various phases of the Project whenever required due to scope change that may arise due to business, delivery or statutory/regulatory reasons;

d) Purchaser shall provide the data (including in electronic form wherever available) to be migrated.

e) To authorize the Managed Service Provider to interact for execution of the Project with external entities such as the other Government Departments, state treasury, authorized banks, trademark database, etc.

f) Provide prompt deliverable feedback: Within <21 working days> from the submission of a deliverable/SLA and performance reports, the Purchaser shall provide a sign offs on the deliverable or its comments for changes.

17.7 Obligations of the Managed Service Provider

a) It shall provide to the Purchaser or its nominated agencies, the Deliverables as specified by the Purchaser.

b) The key obligations and roles & responsibilities of the Managed Service Provider is specified in the document named "Guidelines for Managed Service Providers Offering Cloud Services through Government e-Marketplace (GeM)".

c) It shall perform the Services in a good and workmanlike manner commensurate with industry and technical standards which are generally in effect for international projects and innovations pursuant thereon similar to those contemplated by this Agreement, and so as to comply with the applicable Service Levels.

d) It shall ensure that the Services are being provided as per the Project Timelines set out by the Purchaser.

17.8 Approvals and Required Consents

a) The Parties shall cooperate to procure, maintain and observe all relevant and regulatory and governmental licenses, clearances and applicable approvals (hereinafter the "Required Consents") necessary for the Managed Service Provider to provide the Services. The costs of such Approvals shall be borne by the Party normally responsible for such costs according to local custom and practice in the locations where the Services are to be provided.

b) The Purchaser or its nominated agencies shall use reasonable endeavors to assist Managed Service Provider to obtain the Required Consents (or vice versa, depending on the Scope of work). In the event that any Required Consent is not obtained, the Managed Service Provider and the Purchaser or its nominated agencies will co-operate with each other in achieving a reasonable alternative arrangement as soon as reasonably practicable for the Purchaser or its nominated agencies to continue to process its work with as minimal interruption to its business operations as is commercially reasonable until such Required Consent is obtained, provided that the Managed Service Provider shall not be relieved of its obligations to provide the Services and to achieve the Service Levels until the Required Consents are obtained if and to the extent that the Managed Service Provider's obligations are not dependent upon such Required Consents.

17.9 Use of Assets by the Managed Service Provider

During the Term, the Managed Service Provider shall:

a) take all reasonable and proper care of the entire hardware and software, network or any other information technology infrastructure components used for the Project and other facilities leased / owned / operated by the Managed Service Provider exclusively in terms of ensuring their usability for the delivery of the Services as per this Agreement (hereinafter the "Assets") in proportion to their use and control of such

Assets; and

b) keep all the tangible Assets in as good and serviceable condition (reasonable wear and tear excepted) as at the date the Managed Service Provider takes control of and/or first uses the Assets and during the entire Term of the Agreement.

c) ensure that any instructions or manuals supplied by the manufacturer of the Assets for use of the Assets and which are provided to the Managed Service Provider will be followed by the Managed Service Provider and any person who will be responsible for the use of the Assets;

d) take such steps as may be properly recommended by the manufacturer of the Assets and notified to the Managed Service Provider or as may, in the reasonable opinion of the Managed Service Provider, be necessary to use the Assets in a safe manner;

e) ensure that the Assets that are under the control of the Managed Service Provider, are kept suitably housed and in conformity with Applicable Law;

f) procure permission from the Purchaser or its nominated agencies and any persons duly authorized by them to enter any land or premises on which the Assets are for the time being sited so as to inspect the same, subject to any reasonable third party requirements;

g) not knowingly or negligently use or permit any of the Assets to be used in contravention of any statutory provisions or regulation or in any way contrary to Applicable Law.

17.10 Access to the Purchaser or its Nominated Agencies' Locations

a) For so long as the Managed Service Provider provides services to the Purchaser or its nominated agencies' location, as the case may be, on a non-permanent basis and to the extent necessary, the Purchaser as the case may be or its nominated agencies shall, subject to compliance by the Managed Service Provider with any safety and security guidelines which may be provided by the Purchaser as the case may be or its nominated agencies and notified to the Managed Service Provider in writing, provide the Service Provider with:

(i) reasonable access, in the same manner granted to the Purchaser or its nominated agencies employees, to the Purchaser's location as the case may be

(ii) reasonable work space, access to office equipment as mutually agreed and other related support services in such location and at such other Purchaser's location, as the case may be, as may be reasonably necessary for the Managed Service Provider to perform its obligations hereunder and under the SLA.

b) Access to locations, office equipments and services shall be made available to the Managed Service Provider on an "as is, where is" basis / in appropriate working condition (as per scope of work defined by the Purchaser as the case may be or its nominated agencies. The Managed Service Provider agrees to ensure that its employees, agents and contractors shall not use the location, services and equipment for the following purposes:

(i) for the transmission of any material which is defamatory, offensive or abusive or of an obscene or menacing character; or

(ii) in a manner which constitutes a violation or infringement of the rights of any person, firm or company (including but not limited to rights of copyright or confidentiality).

17.11 Management Phase

17.11.1 Governance

The review and management process of this Agreement shall be carried out in accordance with the Governance Schedule set out in Schedule I of this Agreement and shall cover all the management aspects of the Project.

17.11.2 Use of Services

a) The Purchaser as the case may be or its nominated agencies, will undertake and use the Services in accordance with any instructions or procedures as set out in this Agreement or any agreement that may be entered into between the Parties from time to time;

b) The Purchaser as the case may be or its nominated agencies shall be responsible for the operation and use of the Deliverables resulting from the Services.

17.11.3 Changes

Unless expressly dealt with elsewhere in this Agreement, any changes under or to this Agreement shall be dealt with in accordance with the Change Control Schedule set out in Schedule II of this Agreement.

17.11.4 Security and Safety

a) The Managed Service Provider shall comply with the technical requirements of the relevant security, safety and other requirements specified in the Information Technology Act or Telegraph Act including the regulations issued by Dept. of Telecom (wherever applicable), IT Security Manual of the Purchaser and follow the industry standards related to safety and security, insofar as it applies to the provision of the Services.

b) Each Party to the Agreement shall also comply with Purchaser or the Government of India, and the respective State's security standards and policies in force from time to time at each location of which Purchaser or its nominated agencies make the Managed Service Provider aware in writing insofar as the same apply to the provision of the Services.

c) The Parties to the Agreement shall use reasonable endeavors to report forthwith in writing to each other all identified attempts (whether successful or not) by unauthorized persons (including unauthorized persons who are employees of any Party) either to gain access to or interfere with the Purchaser as the case may be or any of their nominees data, facilities or Confidential Information.

d) The Managed Service Provider shall upon reasonable request by the Purchaser as the case may be or their nominee(s) participate in regular meetings when safety and information technology security matters are reviewed.

e) As per the provisions of this Agreement, the Managed Service Provider shall promptly report in writing to the Purchaser or its nominated agencies, any act or omission which they are aware that could have an adverse effect on the proper conduct of safety and information technology security at the facilities of Purchaser as the case may be.

17.11.5 Cooperation

Except as otherwise provided elsewhere in this Agreement, each Party (“Providing Party”) to this Agreement undertakes promptly to provide the other Party (“Receiving Party”) with all such information and co-operation which the Receiving Party reasonably requests, provided that such information and co-operation:

a) does not require material expenditure by the Providing Party to provide the same;

b) is reasonably required by the Receiving Party in order for it to comply with its obligations under this Agreement;

c) cannot be construed to be Confidential Information; and

d) is capable of being provided by the Providing Party.

17.12 Financial Matters

17.12.1 Terms of Payment

The Cloud Services Bouquet prepared by MeitY allows Government Departments to procure Cloud Services on hourly, monthly or yearly basis (pricing model). The Government Department, for its most suitable pricing model, shall discover the individual unit prices of each of the Cloud Services for the total duration of the project. The Government Department, irrespective of the pricing models, shall pay to the Managed Service Provider for the actual consumption of the Cloud Services.

a) The Managed Managed Service Provider shall provide, in the Commercial Proposal, the individual prices of each of the Cloud Services, specified by the Purchaser, for the total duration of the project.

b) The Purchaser shall pay to the Managed Service Provider for the actual consumption of the Cloud Services during the project duration, and not on the basis of the project duration.

c) The Managed Service Provider shall not increase the fee of the Cloud Services being consumed by the Purchaser during the entire duration of the project, unless there is an agreed provision in the Cloud Contract.

d) The Managed Service Provider shall be responsible, as required under applicable law, for identifying and paying all taxes and other governmental fees and charges (and any penalties, interest, and other additions thereto) that are imposed on it upon or with respect to the transactions and payments under this Contract.

e) The Purchaser may make payment to the Managed Service Provider at the end of the month, quarter or year based on the actual usage of the services and as per the “Unit Costs” discovered under the Commercial Proposal.

f) In consideration of the Services and subject to the provisions of this Agreement, the Purchaser shall pay the Managed Service Provider for the Services rendered in pursuance of this Agreement.

g) Payments shall be subject to the application of liquidated damages or SLA penalties and its adjustments/corrections as may be provided for in the Agreement and the SLA.

h) Save and except as otherwise provided for herein or as agreed between the Parties in writing, the Purchaser shall not be required to make any payments in respect of the Services (or, without limitation to the foregoing, in respect of the Managed Service Provider performance of any obligations under this Agreement or the SLA) other than those covered in this Agreement.

17.12.2 Invoicing and Settlement

i Subject to the specific terms of the Agreement and the SLA, the Managed Service Provider shall submit its invoices in accordance with the following principles:

(i) The Purchaser shall be invoiced by the Managed Service Provider for the Services. Generally and unless otherwise agreed in writing between the Parties or expressly set out in the SLA, the Managed Service Provider shall raise an invoice as per this Agreement; and

(ii) Any invoice presented in accordance with this Clause shall be in a form agreed with the Purchaser.

ii The Managed Service Provider alone shall invoice all payments after receiving due approval of completion of payment milestone from the competent authority. Such invoices shall be accurate with all adjustments or changes in the terms of payment. The Managed Service Provider shall waive any charge for a Service that is not invoiced within six months after the end of the month in which the change relating to such Service is (i) authorized or (ii) incurred, whichever is later.

iii Payment shall be made within <30 working days> of the receipt of invoice along with supporting documents by the Purchaser subject to deduction of applicable liquidated damages or SLA penalties. The penalties are imposed on the Managed Service Provider as per the SLA criteria specified in the SLA.

iv The Purchaser shall be entitled to delay or withhold payment of any invoice or part of it delivered by the Managed Service Provider where the Purchaser disputes/withholds such invoice or part of it provided that such dispute is bona fide. The withheld amount shall be limited to that which is in dispute. The disputed / withheld amount shall be settled in accordance with the escalation procedure as set out in this Agreement. Any exercise by the Purchaser under this Clause shall not entitle the Managed Service Provider to delay or withhold provision of the Services.

v The Managed Service Provider shall be solely responsible to make payment to its sub-contractors, if they are expressly approved by the Purchaser to work with the Managed Service Provider.

17.12.3 Tax

a) The Purchaser or its nominated agencies shall be responsible for withholding taxes from the amounts due and payable to the Managed Service Provider wherever applicable. The Managed Service Provider shall pay for all other taxes in connection with this Agreement, SLA, scope of work and any other engagement required to be undertaken as a part of this Agreement, including, but not limited to property, sales, use, excise, value-added, goods and services, consumption and other similar taxes or duties.

b) The Purchaser or its nominated agencies shall provide Managed Service Provider with the original tax receipt of any withholding taxes paid by Purchaser or its nominated agencies on payments under this Agreement. The Managed Service Provider agrees to reimburse and hold the Purchaser or its nominated agencies harmless from any deficiency including penalties and interest relating to taxes that are its responsibility under this paragraph. For purposes of this Agreement, taxes shall include taxes incurred on transactions between and among the Purchaser or its nominated agencies, the Managed Service Provider and third party subcontractors, if any.

c) The Parties shall cooperate to enable each Party to accurately determine its own tax liability and to minimize such liability to the extent legally permissible. In connection therewith, the Parties shall provide each other with the following:

(i) any resale certificates;

(ii) any relevant information regarding out-of-state or use of materials, equipment or services; and

(iii) any direct pay permits, exemption certificates or information reasonably requested by the other Party.

17.13 Termination

17.13.1 For Material Breach

a) In the event that either Party believes that the other Party is in Material Breach of its obligations under this Agreement, such aggrieved Party may terminate this Agreement upon giving a one month’s notice for curing the Material Breach to the other Party. In case the Material Breach continues, after the notice period, the Purchaser or Managed Service Provider, as the case may be will have the option to terminate the Agreement. Any notice served pursuant to this Clause shall give reasonable details of the Material Breach, which could include the following events and the termination will become effective:

(i) Managed Service Provider becomes insolvent, bankrupt, resolution is passed for the winding up of the Managed Service Provider’s organization;

(ii) Information provided to the Purchaser is found to be incorrect;

(iii) Contract conditions are not met as per the requirements specified in the application document;

(iv) Misleading claims about the empanelment status with MeitY are made;

(v) If the Managed Service Provider fails to perform any other obligation(s) under the Agreement

(vi) If the Managed Service Provider is not able to deliver the services as per the SLAs which translates into Material Breach, then the Purchaser may serve a 30 days written notice for curing this Material Breach. In case the Material Breach continues, after the expiry of such notice period, the Purchaser will have the option to terminate this Agreement. Further, the Purchaser may offer a reasonable opportunity to the Managed Service Provider to explain the circumstances leading to such a breach.

b) In the event, the Purchaser terminates the Agreement in whole or in part, the Purchaser may procure, upon such terms and conditions as it deems appropriate, services similar to those undelivered, and the Managed Service Provider shall be liable to the Purchaser for any excess costs for such similar services where such excess costs shall not exceed 10% of the value of the undelivered services. However, the Managed Service Provider shall continue to work with the Purchaser to the extent not terminated. On termination, the exit management and transition provisions as per the Agreement will come into effect.

c) The Purchaser may by giving a one month's written notice, terminate this Agreement if a change of control of the Managed Service Provider has taken place. For the purposes of this Clause, in the case of Managed Service Provider, change of control shall mean the events stated in Clause 1.4, and such notice shall become effective at the end of the notice period as set out in Clause 1.4.

d) In the event that Managed Service Provider undergoes such a change of control, Purchaser may, as an alternative to termination, require a full Performance Guarantee for the obligations of Managed Service Provider by a guarantor acceptable to Purchaser or its nominated agencies. If such a guarantee is not furnished within 30 days of Purchaser's demand, the Purchaser may exercise its right to terminate this Agreement in accordance with this Clause by giving 15 days further written notice to the Managed Service Provider.

e) The termination provisions set out in this Clause shall apply mutatis mutandis to the SLA.

17.13.2 Termination for Convenience

a) The Purchaser may at any time terminate the Contract for any reason by giving the Managed Service Provider a notice of termination that refers to this clause.

b) Upon receipt of the notice of termination under this clause, the Managed Service Provider shall either as soon as reasonably practical or upon the date specified in the notice of termination:

(i) cease all further work, except for such work as the Purchaser may specify in the notice of termination for the sole purpose of protecting that part of the system/application/solution already executed, or any work required to leave
the site in a clean and safe condition;

(ii) terminate all subcontracts, if any, except those to be assigned to the Purchaser pursuant to Clause 1.13.2 (d) (ii) below;

c) remove all Managed Service Provider's equipment from the site, repatriate the Managed Service Provider's and its Subcontractors' personnel, if any, from the site, remove from the site any wreckage, rubbish, and debris of any kind;

d) in addition, the Managed Service Provider shall:

(i) deliver to the Purchaser the parts of the system/application/solution executed by the Managed Service Provider up to the date of termination;

(ii) to the extent legally possible, assign to the Purchaser all right, title, and benefit of the Managed Service Provider to the system/subsystem/application/solution/, as at the date of termination, and, as may be required by the Purchaser, in any subcontracts, if any, concluded between the Managed Service Provider and its Subcontractors;

(iii) deliver to the Purchaser all non-proprietary drawings, specifications, and other documents prepared by the Managed Service Provider or its Subcontractors, if any, as of the date of termination in connection with the system/application/solution.

17.13.3 Effects of termination

a) In the event that Purchaser terminates this Agreement pursuant to failure on the part of the Managed Service Provider to comply with the conditions as contained in this Clause and depending on the event of default, Performance Guarantee, if any, furnished by Managed Service Provider may be forfeited.

b) Upon termination of this Agreement, the Parties will comply with the Exit Management Plan as set out in the RFP. Termination of this Agreement due to Bankruptcy of Managed Service Provider

The Purchaser may serve written notice on Managed Service Provider at any time to terminate this Agreement with immediate effect in the event that the Managed Service Provider reporting an apprehension of bankruptcy to the Purchaser or its nominated agencies

17.14 Indemnification & Limitation of Liability

a) Subject to Clause 1.14 (d) below, Managed Service Provider (the "Indemnifying Party") undertakes to indemnify, hold harmless the Purchaser (the "Indemnified Party") from and against all claims, liabilities, losses, expenses (including reasonable attorneys' fees), fines, penalties, taxes or damages (Collectively “Loss”) on account of bodily injury, death or damage to tangible personal property arising in favor of any person, corporation or other entity (including the Indemnified Party) attributable to the Indemnifying Party's negligence or willful default in performance or non-performance under this Agreement.

b) If the Indemnified Party promptly notifies Indemnifying Party in writing of a third party claim against Indemnified Party that any Service provided by the Indemnifying Party infringes a copyright, trade secret or patents incorporated in India of any third party, Indemnifying Party will defend such claim at its expense and will pay any costs or damages, that may be finally awarded against Indemnified Party.

c) Indemnifying Party will not indemnify the Indemnified Party, however, if the claim of infringement is caused by

(i) Indemnified Party’s misuse or modification of the Service;

(ii) Indemnified Party’s failure to use corrections or enhancements made available by the Indemnifying Party;

(iii) Indemnified Party’s use of the Service in combination with any product or information not owned or developed by Indemnifying Party;

However, if any service, information, direction, specification or materials provided by Indemnified Party or any third party contracted to it, is or likely to be held to be infringing, Indemnifying Party shall at its expense and option either

(i) Procure the right for Indemnified Party to continue using it

(ii) Replace it with a no infringing equivalent

(iii) Modify it to make it no infringing.

The foregoing remedies constitute Indemnified Party's sole and exclusive remedies and Indemnifying Party's entire liability with respect to infringement.

d) The indemnities set out in Clause 1.14 shall be subject to the following conditions:

(i) the Indemnified Party as promptly as practicable informs the Indemnifying Party in writing of the claim or proceedings and provides all relevant evidence, documentary or otherwise;

(ii) the Indemnified Party shall, at the cost of the Indemnifying Party, give the Indemnifying Party all reasonable assistance in the Defense of such claim including reasonable access to all relevant information, documentation and personnel provided that the Indemnified Party may, at its sole cost and expense, reasonably participate, through its attorneys or otherwise, in such Defense;

(iii) if the Indemnifying Party does not assume full control over the Defense of a claim as provided in this Article, the Indemnifying Party may participate in such Defense at its sole cost and expense, and the Indemnified Party will have the right to defend the claim in such manner as it may deem appropriate, and the cost and expense of the Indemnified Party will be included in Losses;

(iv) the Indemnified Party shall not prejudice, pay or accept any proceedings or claim, or compromise any proceedings or claim, without the written consent of the Indemnifying Party;

(v) all settlements of claims subject to indemnification under this Clause will:

(a) be entered into only with the consent of the Indemnified Party, which consent will not be unreasonably withheld and include an unconditional release to the Indemnified Party from the claimant or plaintiff for all liability in respect of such claim; and

(b) include any appropriate confidentiality agreement prohibiting disclosure of the terms of such settlement;

(vi) the Indemnified Party shall account to the Indemnifying Party for all awards, settlements, damages and costs (if any) finally awarded in favor of the Indemnified Party which are to be paid to it in connection with any such claim or proceedings;

(vii) the Indemnified Party shall take steps that the Indemnifying Party may reasonably require to mitigate or reduce its loss as a result of such a claim or proceedings;

(viii) in the event that the Indemnifying Party is obligated to indemnify an Indemnified Party pursuant to this Article, the Indemnifying Party will, upon payment of such indemnity in full, be subrogated to all rights and defenses of the Indemnified Party with respect to the claims to which such indemnification relates; and

(ix) if a Party makes a claim under the indemnity set out under Clause 1.14 (a) above in respect of any particular Loss or Losses, then that Party shall not be entitled to make any further claim in respect of that Loss or Losses (including any claim for damages).

e) The liability of either Party (whether in contract, tort, negligence, strict liability in tort, by statute or otherwise) for any claim in any manner related to this Agreement, including the work, deliverables or Services covered by this Agreement, shall be the payment of direct damages only which shall in no event exceed one time the total contract value payable under this Agreement. The liability cap given under this Clause shall not be applicable to the indemnification obligations set out in Clause 1.14 and breach of Clause 1.11.4.

f) In no event shall either party be liable for any consequential, incidental, indirect, special or punitive damage, loss or expenses (including but not limited to business interruption, lost business, lost profits, or lost savings) nor for any third party claims (other than those set-forth in Clause 1.14 (a) even if it has been advised of their possible existence.

g) The allocations of liability in this Section 1.14 represent the agreed and bargained-for understanding of the parties and compensation for the Services reflects such allocations. Each Party has a duty to mitigate the damages and any amounts payable under an indemnity that would otherwise be recoverable from the other Party pursuant to this Agreement by taking appropriate and commercially reasonable actions to reduce or limit the amount of such damages or amounts.

17.15 Force Majeure

(i) Definition of Force Majeure

a. “Force Majeure” shall mean any event beyond the reasonable control of either Party, as the case may be, and which is unavoidable notwithstanding the reasonable care of the Party affected.

(ii) Force Majeure events

A Force Majeure shall include, without limitation, the following:

a. war, hostilities, or warlike operations (whether a state of war be declared or not), invasion, act of foreign enemy, and civil war;

b. strike, lockout (strike and lockout not caused due to either Party’s default), sabotage embargo, import restriction, port congestion, lack of usual means of public transportation and communication, industrial dispute, shipwreck, shortage or restriction of power supply, epidemics, quarantine, and plague;

c. earthquake, landslide, volcanic activity, fire, flood or inundation, tidal wave, typhoon or cyclone, hurricane, storm, lightning, or other inclement weather condition, nuclear and pressure waves, or other natural or physical disaster;

(iii) If either party is prevented, hindered, or delayed from or in performing any of its obligations under the Contract by an event of Force Majeure, then it shall notify the other in writing of the occurrence of such event and the circumstances of the event of Force Majeure within five (5) days after the occurrence of such event.

(iv) The party who has given such notice shall be excused from the performance or punctual performance of its obligations under the Contract for so long as the relevant event of Force Majeure continues and to the extent that such party's performance is prevented, hindered, or delayed. The time for achieving Final Acceptance shall be extended.

(v) The party or parties affected by the event of Force Majeure shall use reasonable efforts to mitigate the effect of the event of Force Majeure upon its or their performance of the Contract and to fulfill its or their obligations under the Contract, but without prejudice to either party's right to terminate the Contract.

(vi) No delay or nonperformance by either party to this Contract caused by the occurrence of any event of Force Majeure shall:

a. constitute a default or breach of the Contract;
b. give rise to any claim for damages or additional cost or expense occasioned by the delay or nonperformance, if, and to the extent that, such delay or nonperformance is caused by the occurrence of an event of Force Majeure.

(vii) If the performance of the Contract is substantially prevented, hindered, or delayed for a single period of more than sixty (60) days on account of one or more events of Force Majeure during the time period covered by the Contract, the parties will attempt to develop a mutually satisfactory solution, failing which, either party may terminate the Contract by giving a notice to the other.

(viii) In the event of termination pursuant to material breach, the rights and obligations of the Managed Service Provider and Purchaser shall be as specified in the clause titled Termination.

(ix) For the avoidance of doubt, it is expressly clarified that the failure on the part of the selected Managed Service Provider under this Agreement or the service levels to implement any disaster contingency planning and back-up and other data safeguards in accordance with the terms of this Agreement or the service levels against natural disaster, fire, sabotage or other similar occurrence shall not be deemed to be a Force Majeure event. For the avoidance of doubt, it is further clarified that any negligence in performance of Services which directly causes any breach of security like hacking aren't the forces of nature and hence wouldn't be qualified under the definition of "Force Majeure". In so far as applicable to the performance of Services, Managed Service Provider will be solely responsible to complete the risk assessment and ensure implementation of adequate security hygiene, best practices, processes and technology to prevent any breach of security and any resulting liability therefrom (wherever applicable).

(x) For the Managed Service Provider to take benefit of this clause, it is a condition precedent that the Managed Service Provider must promptly notify Purchaser, in writing of such conditions and the cause thereof within five calendar days of the arising of the Force Majeure event. Purchaser, or the consultant / committee appointed by Purchaser shall study the submission of the Managed Service Provider and inform whether the situation can be qualified one of Force Majeure. Unless otherwise directed by Purchaser in writing, the Managed Service Provider shall continue to perform its obligations under the resultant Agreement as far as it is reasonably practical, and shall seek all reasonable alternative means for performance of services not prevented by the existence of a Force Majeure event.

(xi) In the event of delay in performance attributable to the presence of a force majeure event, the time for performance shall be extended by a period(s) equivalent to the duration of such delay. If the duration of delay continues beyond a period of 30 days, Purchaser and the Managed Service Provider shall hold consultations with each other in an endeavor to find a solution to the problem.

Notwithstanding anything to the contrary mentioned above, the decision of Purchaser shall be final and binding on the Managed Service Provider.

17.16 Adherence to the Empanelment Terms & Conditions

The Managed Service Provider shall ensure that the underlying Cloud Managed Service Provider is adhering to all the terms and conditions specified in the MeitY's CSP Empanelment RFP at all times during the tenure of the Purchaser's project.

17.17 Information Security

One of the most critical issues that need to be addressed in the Cloud Contract / Agreement is the security of the data and application. The level of sensitivity of data requires different controls to be put in place in the Cloud to prevent a compromise.

17.17.1 Compliances and Certifications

(i) As part of the empanelment process, MeitY has mandated CSPs to have following certifications.

a. ISO 27001:2013 – Information security management systems requirements (Data Center and the Cloud Services should be certified for the ISO 27001 standard)

b. ISO 20000:1 - Service management system requirements (NOC and SOC offered for the Data Center and the managed services quality should be certified for ISO 20000:1)

c. ISO 27017 - Code of practice for information security controls based on ISO/IEC 27002 for Cloud Services

d. ISO 27018 - Code of practice for protection of Personally Identifiable Information (PII) in Public Clouds acting as PII processors

e. TIA-942-B / UPTIME (Tier III or higher) – Data centre standard covering site space and layout, cabling infrastructure, tiered reliability and environmental considerations

The Managed Service Provider shall ensure the sustenance of the above certificates and compliances applicable to the underlying CSPs during the entire duration of the project. The Managed Service Provider is required to possess and sustain following certifications in addition to ensuring the sustenance of the above certificates and compliances applicable to the underlying CSP during the entire duration of the project.

a. ISO 27001:2013 – Information security management systems requirements

b. ISO 20000:1 - Service management system requirements

(ii) If the Purchaser has financial and payment related data that is proposed to be hosted on the Cloud, the Managed Service Provider shall provide Payment Card Industry Data Security Standard (PCI DSS) compliant technology infrastructure of underlying CSP for storing, processing, and transmitting payment related information in the Cloud. This standard is required if the transactions involve credit card payments.

(iii) CSPs are audited by STQC regularly for the requirements specified in the CSPs Empanelment RFP and for other guidelines & security requirements specified by MeitY or any standards body setup / recognized by Government of India from time to time and notified to the CSPs.

a. The Managed Service Provider shall ensure that the underlying CSP complies or meets any security requirements applicable to it either published (or to be published) by MeitY or the Purchaser or any standards body setup / recognized by Government of India from time to time and notified to the Managed Service Provider / MeitY empaneled CSP as a mandatory guideline / standard.

b. The Managed Service Provider shall meet all the security requirements indicated in the IT Act 2000 and rules & regulations as amended from time to time. The underlying CSP shall meet all terms and conditions of the Empanelment of Cloud Service Offerings of Cloud Managed Service Providers and shall continuously comply with the audit criteria defined by STQC.

17.17.2 Privacy and Security Safeguards

(i) The Managed Service Provider shall implement reasonable and appropriate measures to secure the Purchaser’s data and content against accidental or unlawful loss, access or disclosure.

(ii) If the data is classified as sensitive / confidential / restricted, the Managed Service Provider shall ensure that the data is encrypted as part of a standard security process for sensitive / confidential / restricted content or choose the right cryptographic algorithms evaluating security, performance, and compliance requirements specific to the Purchaser’s application and may choose from multiple key management options approved by the Purchaser.

(iii) The Managed Service Provider shall notify the Purchaser promptly in the event of security incidents or intrusions, or requests from foreign governments / their agencies for access to the data, to enable the Purchaser to manage these events proactively.

(iv) The Managed Service Provider shall not delete any data at the end of the Agreement/Contract (for a maximum of 45 days beyond the expiry of the Agreement) without the express approval of the Purchaser. After the approval to delete the data is accorded by the Purchaser, the Managed Service Provider shall ensure that all the storage blocks or multiple copies of data, if any, are unallocated or zeroed out so that it cannot be recovered. If due to some regulatory reasons, it is required to securely decommission data, the Purchaser can implement data encryption at rest using Purchaser’s managed keys, which are not stored in the Cloud. Then Purchaser may delete the key used to protect the decommissioned data, making it irrecoverable.

(v) The Managed Service Provider shall report to the Purchaser, in writing, of information security breaches by unauthorized persons (including unauthorized persons who are employees of any Party) either to gain access to or interfere with the Project's Data, facilities or Confidential Information.

(vi) The Managed Service Provider shall undertake to treat information passed on to it under this Agreement/Contract as classified. Such Information shall not be communicated / published / advertised by the Managed Service Provider to any person/organization without the express permission of the Purchaser.

(vii) The Managed Service Provider shall not use/process the service attributes and data associated with Cloud and managed services for the purposes beyond the scope of the current project.

17.17.3 Confidentiality

(i) The Managed Service Provider shall maintain confidentiality, integrity, availability and privacy of the Purchaser data. The Managed Service Provider shall execute NonDisclosure Agreement (NDA) with the Purchaser with respect to this Project. Following information is excluded from the NDA.

a. information already available in the public domain;

b. information which has been developed independently by the Managed
Managed Service Provider;

c. information which has been received from a third party who had the right to disclose the aforesaid information;

d. Information which has been disclosed to the public pursuant to a court order.

(ii) The subcontractors, other than the Managed Service Provider, after the express approval by the Purchaser, shall be permitted to obtain the Purchaser’s data only to deliver the services the Managed Service Provider has retained them to provide and shall be prohibited from using the Purchaser’s data for any other purpose. The Managed Service Provider must take express approval of the Purchaser to use the services of subcontractor(s). The Managed Service Provider remains responsible for its subcontractors’ compliance with Managed Service Provider’s obligations under the Project.

(iii) Disclosure of any part of the non-public information to parties not directly involved in providing the services requested, unless required to do so by the Court of Law within India or other Statutory Authorities of Indian Government, could result in premature termination of the Agreement. The Purchaser may apart from blacklisting the Managed Service Provider, initiate legal action against the Managed Service Provider as per the applicable laws of India. The Managed Service Provider shall also not make any news release, public announcements, use of trademark or logo or any other reference on the Project, including application document / RFP, without obtaining prior written consent from the Purchaser.

(iv) The Managed Service Provider shall notify the Purchaser as soon as possible in the event of an actual or suspected breach of data.

(v) The Managed Service Provider shall keep confidential all the details and information with regard to the Project, including systems, facilities, operations, management and maintenance of the systems/facilities.

(vi) The Purchaser or its nominated agencies shall retain all rights to prevent, stop and if required take the necessary punitive action against the Managed Service Provider regarding any forbidden disclosure.

(vii) The Managed Service Provider shall ensure that all its employees, agents and subcontractors involved in the Project, execute individual non-disclosure agreements, which have been duly approved by the Purchaser with respect to this Project. The Managed Service Provider may submit a declaration that it has obtained the NDA from its employees. However, if the project is critical in nature, Managed Service Provider may get NDAs signed from every resource involved in the project and submit it to Purchaser (Optional).

(viii) Any handover of the confidential information needs to be maintained in a list, both by Purchaser & Managed Service Provider, containing at the very minimum, the name of provider, recipient, date of generation of the data, date of handing over of data, mode of information, purpose and signatures of both parties.

(ix) Notwithstanding anything to the contrary mentioned hereinabove, the Managed Service Provider shall have the right to share the Letter of Intent / work order provided to it by the Purchaser in relation to this Agreement, with its prospective purchasers solely for the purpose of and with the intent to evidence and support its work experience under this Agreement.

17.17.4 Location of Data

(i) The Managed Service Provider shall offer Cloud Services to the Purchaser from a MeitY empaneled data centre of the underlying CSP which is located within India.

(ii) The Managed Service Provider shall store all types of data (including but not limited to account & user access data, text, audio, video, image, software, machine image, and any computational results that the Purchaser or any end user derives through their use of the Managed Service Provider’s services) within the Indian Territory and as per the terms and conditions specified in the CSP’s Empanelment RFP; and shall not take out / allow to take out any kind of data outside of India unless it is explicitly approved by the Purchaser.

(iii) E-Discovery: Electronic discovery (e-Discovery) is the process of locating, preserving, collecting, processing, reviewing, and producing Electronically Stored Information (ESI) in the context of criminal cases, legal proceedings or investigation. The Managed Service Provider shall ensure that the Purchaser/any other agency authorized by the Purchaser is able to access and retrieve such data in the underlying CSP environment in a timely fashion.

(iv) Law Enforcement Request: The Law Enforcement Agency, as mandated under any law of India for the time being in force, may seek access to information stored on Cloud as provided by the Managed Service Provider. The onus shall be on the Managed Service Provider to perform all due diligence before releasing any such information to any such Law Enforcement Agency of India.

17.18 Audit, Access and Reporting

CSPs offer a variety of Cloud Services. However, all Cloud Services have not been empaneled with MeitY. Those Cloud Services which have been empaneled with MeitY have been audit by STQC against a set of audit criteria prepared by it, which are drawn from the CSPs Empanelment RFP and include technical, security and legal requirements, among others.

(i) The Managed Service Provider shall ensure that the underlying CSP's service offerings comply with the audit requirements specified by MeitY/STQC through the CSPs Empanelment RFP or any other mechanism.

(ii) The Purchaser or its nominated agency shall have the right to audit and inspect Managed Service Provider, agents and third party facilities, data centres, documents, records, procedures and systems relating to the provision of the services, but only to the extent that they relate to the provision of the services, as shall be reasonably necessary to verify:

a. The security, integrity and availability of all data processed, held or conveyed by the Managed Service Provider on behalf of the Purchaser and documentation related thereto;

b. That the actual level of performance of the services is the same as specified in the SLA;

c. That the Managed Service Provider has complied with the relevant technical standards, and has adequate internal controls in place; and

d. The compliance of the Managed Service Provider with any other obligation under the MSA and SLA.

(iii) The Managed Service Provider shall be required to demonstrate compliance to all the requirements, guidelines, standards, etc., specified in the CSPs Empanelment RFP prepared by MeitY, as and when required by the Purchaser.

(iv) In addition to the STQC audit conducted as per the empanelment of Cloud Service Offerings of CSP with MeitY, the Managed Service Provider shall allow the Purchaser / any agency authorized by the Purchaser to conduct audit of its services including underlying CSP's Cloud environment.

17.19 Intellectual Property Rights

c) The Purchaser shall own and have a right in perpetuity to use all newly created Intellectual Property Rights which have solely arisen out of or have been developed solely during execution of this Agreement, including but not limited to all processes, products, specifications, reports, drawings and other documents which have been newly created and developed by the Managed Service Provider solely during the performance of the Services. The Managed Service Provider undertakes to disclose all such Intellectual Property Rights arising in performance of the Services to the Purchaser and execute all such agreements/documents and file all relevant applications, effect transfers and obtain all permits and approvals that may be necessary in this regard to effectively transfer and conserve the Intellectual Property Rights of the Purchaser.

d) Further, the Managed Service Provider shall be obliged to ensure that all approvals, registrations, licenses, permits and rights which are, inter-alia, necessary for use of the Deliverables, applications, services, etc. provided by the Managed Service Provider under this Agreement shall be acquired in the name of the Purchaser, prior to termination of this Agreement and which shall be assigned by the Purchaser to the Managed Service Provider for the purpose of execution of any of its obligations under the terms of this Agreement. However, subsequent to the term of this Agreement, such approvals, etc., shall endure to the exclusive benefit of the Purchaser.

e) Pre-existing work: All intellectual property rights existing prior to the Effective Date of this Agreement shall belong to the Party that owned such rights immediately prior to the Effective Date. Subject to the foregoing, the Purchaser will also have rights to use and copy all process, specifications, reports and other document drawings, manuals, and other documents provided by Managed Service Provider as part of the scope of work under this Agreement for the purpose of this Agreement on non-exclusive, nontransferable, perpetual, royalty-free license to use basis.

f) Ownership of documents: The Purchaser shall own all documents provided by or originating from the Purchaser and all documents produced by or from or for the Managed Service Provider in the course of performing the Services. Forthwith upon expiry or earlier termination of this Agreement and at any other time on demand by the Purchaser, the Managed Service Provider shall deliver to the Purchaser all documents provided by or originating from the Purchaser and all documents produced by or from or for the Managed Service Provider in the course of performing the Services, unless otherwise directed in writing by the Purchaser at no additional cost. The Managed Service Provider shall not, without the prior written consent of the Purchaser store, copy, distribute or retain any such Documents.

g) The ownership of all IPR rights in any and all documents, artefacts, etc. (including all training materials) made during the Term for implementation of the Project under this Agreement will lie with Purchaser.

h) Notwithstanding anything contained herein, the Managed Service Provider may use in its business activities the ideas, concepts and know-how which are retained in the unaided memories of its employees who have worked in the Project under this Agreement. The foregoing does not permit intentional memorization of the any information for the purpose of evading obligations contained in this Agreement.

17.20 Liquidated Damages

Time is the essence of the Agreement and the delivery dates are binding on the Managed Service Provider. In the event of delay or any gross negligence in implementation of the Project, for causes solely attributable to the Selected Managed Service Provider, in meeting the deliverables, the Purchaser shall be entitled at its option to recover from the Managed Service Provider as agreed, liquidated damages, a sum of <0.5%> of the value of the deliverable which suffered delay or gross negligence for each completed week or part thereof subject to a limit of <10%> of the total contract value. This right to claim any liquidated damages shall be without prejudice to other rights and remedies available to Purchaser under the contract and law. Once the maximum deduction is reached, the Purchaser may consider termination of the Contract.

17.21 Insurance Cover

17.21.1 Obligation to Maintain Insurance

(i) In connection with the provision of the Services, the Managed Service Provider must have and maintain:

a) for the Agreement Period, valid and enforceable insurance coverage for: (i) public liability;

(ii) either professional indemnity or errors and omissions;

(iii) workers' compensation as required by law; and

(iv) any additional types, if any ; and

(ii) for <one> year following the expiry or termination of the Agreement, valid and enforceable insurance policies (if relevant).

17.21.2 Certificates of currency

The Managed Service Provider must, on request by the Purchaser, provide current relevant confirmation of insurance documentation from its insurance brokers certifying that it has insurance as required by this Clause 1.21. The Managed Service Provider agrees to replace any coverage prior to the date of expiry/cancellation.

17.21.3 Non-compliance

Purchaser or its nominated agencies may, at its election, terminate this Agreement as per Clause 1.13, upon the failure of Managed Service Provider or notification of such failure, to maintain the required insurance coverage. Inadequate insurance coverage for any reason shall not relieve Managed Service Provider of its obligations under this Agreement.

17.22 Changes in Cloud Service Offerings

(i) The Managed Service Provider shall inform the Purchaser, at least 3 months in advance, about the material changes that the Managed Service Provider is planning to implement in the Cloud Service being consumed by the Purchaser.

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

17.23 Transitioning/Exit

(i) The Managed Service Provider shall not delete any data at the end of the agreement from the underlying CSP's Cloud environment (for a maximum of 45 days beyond the expiry of the Agreement) without the express approval of the Purchaser. The Purchaser shall pay to the Managed Service Provider the cost associated with retaining the data beyond 45 days. The associated cost shall be arrived at based on the cost figures indicated in the commercial quote submitted by the Managed Service Provider.

(ii) The underlying CSP shall be responsible for providing the tools for import / export of VMs, associated content, data, etc., and the Managed Service Provider, in consultation with the Purchaser, shall be responsible for preparation of the Exit Management Plan and carrying out the exit management / transition related activities.

(iii) The Managed Service Provider shall provide the Purchaser or its nominated agency with a recommended exit management plan ("Exit Management Plan") or transition plan indicating the nature and scope of the underlying CSP’s transitioning services. The Exit Management Plan shall deal with the following aspects of the exit management in relation to the Agreement as a whole or the particular service of the Agreement:

a. Transition of Managed Services
b. Migration from the incumbent Cloud Service Provider’s environment to the new environment

(iv) The Managed Service Provider is responsible for both transition of the services as well as migration of the VMs, Data, Content and other assets to the new environment.

(v) The Managed Service Provider shall carry out the migration of the VMs, data, content and any other assets to the new environment (alternate Cloud Service Provider or Data Centre) identified by the Purchaser to enable successful deployment and running of the Purchaser’s solution in the new environment.

(vi) The format of the data transmitted from the current CSP to the new environment identified by the Department should leverage standard data formats (e.g., OVF, etc.) whenever possible to ease and enhance portability. The format shall be finalized in consultation with the Purchaser.

(vii) The Managed Service Provider shall transition Purchaser’s solution including retrieval of all data in the formats approved by the Purchaser.

(viii) The Managed Service Provider shall ensure that all the documentation required by the Purchaser for smooth transition (in addition to the documentation provided by the underlying Cloud Service Provider) are kept up to date and all such documentation is handed over to the Purchaser during regular intervals as well as during the exit management process.

(ix) The Managed Service Provider shall transfer the organizational structure developed during the term to support the delivery of the Exit Management Services. This will include:

a. Documented and updated functional organization charts, operating level agreements with third-party contractors, phone trees, contact lists, and standard operating procedures.
b. Physical and logical security processes and tools, including catalogues, badges, keys, documented ownership and access levels for all passwords, and instructions for use and operation of security controls.

(x) The Managed Service Provider shall carry out following key activities, including but not limited to, as part of the knowledge transfer:

a. Preparing documents to explain design and characteristics
b. Carrying out joint operations of key activities or services
c. Briefing sessions on processes and documenting processes
d. Sharing the logs, etc.

e. Briefing sessions on the managed services, the way these are deployed on Cloud and integrated

f. Briefing sessions on the offerings (IaaS/PaaS/SaaS) of the underlying Cloud Service Provider

(xi) The Managed Service Provider shall transfer know-how relating to operation and maintenance of the solution, software, Cloud Services, etc.

17.24 Service Level Agreement

Service Level Agreements (SLAs) are an important way of ensuring that the Managed Service Provider is meeting the level of service expected by the Purchaser. The Service Level Agreements (SLAs) mentioned in the document named “Model Service Level Agreements” available on the MeghRaj webpage at

https://www.meity.gov.in/writereaddata/files/Guidelines_User_Department_Procuring_Cloud%20Services_Ver1.0.pdf shall be applicable to Managed Service Provider and is part of this Agreement.

17.25 Suspension

(i) The Managed Service Provider shall not suspend the right to access or use the Cloud Services without providing a written notice, 30 days in advance, to the Purchaser, unless the use of the Cloud service offerings by the Purchaser poses security risk to the Cloud Services being consumed by the Purchaser.

17.26 Conflict of Interest

(i) The Managed Service Provider shall furnish an affirmative statement as to the absence of, actual or potential conflict of interest on the part of the Managed Service Provider or any prospective subcontractor due to prior, current, or proposed contracts, engagements, or affiliations with the Purchaser. Additionally, such disclosure shall address any / all potential elements (time frame for service delivery, resource, financial

or other) that would adversely impact the ability of the Managed Service Provider to complete the requirements as given in the application document / RFP.

17.27 Relationship

The Managed Service Provider is fully responsible for the services performed by it or on its behalf.

(i) Nothing mentioned herein shall be construed as relationship of master and servant or of principal and agent as between the Purchaser and the Managed Service Provider. No partnership shall be constituted between the Purchaser and the Managed Service Provider by virtue of this Agreement nor shall either party have powers to make, vary or release their obligations on behalf of the other party or represent that by virtue of this or any other Agreement a partnership has been constituted, or that it has any such power. The Managed Service Provider shall be fully responsible for the services performed by it or on its behalf.

(ii) The Managed Service Provider shall not use the Purchaser’s name or any service or proprietary name, mark or logo for promotional purpose without first having obtained the Purchaser’s prior written approval.

17.28 Fraud & Corruption

The Managed Service Provider shall observe the highest standards of ethics during the performance and execution of the Project.

(i) The Purchaser shall terminate the Agreement if the Managed Service Provider has been determined by the Purchaser to having been engaged in corrupt, fraudulent, unfair trade practices, coercive or collusive.

(ii) The following terms apply in this context.

a. "Corrupt practice" means offering, giving, receiving or soliciting of anything of value to influence the action of the Purchaser during the tenure of the Project.

b. "Fraudulent practice" means a misrepresentation of facts, in order to influence a procurement process or the execution of a contract, to the Purchaser, and includes collusive practices designed to establish proposal prices at artificially high or non-competitive levels and to deprive the Purchaser of the benefits of free and open competition.

c. “Unfair trade practices” means supply of services different from what is ordered on, or change in the Scope of Work which was agreed to.

d. “Coercive practices” means harming or threatening to harm, directly or indirectly, persons or their property to influence their participation during the period of Project.

e. “Collusive practices” means a scheme or arrangement between two or more prospective Managed Service Providers with or without the knowledge of the Purchaser, designed to establish prices at artificial, non-competitive levels;

17.29 Applicable Law and Dispute Resolution

The terms and conditions of this Agreement shall at all times be construed in accordance with IT Act and Regulations, Privacy laws and other applicable laws of India thereunder as amended from time to time. All legal disputes are subject to the exclusive jurisdiction of (where Purchaser is located) courts only.

(i) Any dispute arising out of or in connection with this Agreement or the SLA shall in the first instance be dealt with in accordance with the escalation procedure as set out in the Agreement.

(ii) In case the escalations do not help in resolution of the problem within 3 weeks (or a duration specified by the Purchaser) of escalation, both the parties should agree on a mediator for communication between the two parties. The process of the mediation would be as follows:

a. Aggrieved party should refer the dispute to the identified mediator in writing, with a copy to the other party. Such a reference should contain a description of the nature of the dispute, the quantum in dispute (if any) and the relief or remedy sought suitable.

b. The mediator shall use its best endeavors to conclude the mediation within a certain number of days of its appointment.

c. If no resolution can be reached through mutual discussion or mediation within 30 days then the matter should be referred to experts for advising on the issue.

(iii) In case the mediation does not help in resolution and it requires expertise to understand an issue, a neutral panel of 3 experts, agreeable to both parties should be constituted. The process of the expert advisory would be as follows:

a. Aggrieved party should write to the other party on the failure of previous alternate dispute resolution processes within the timeframe and requesting for expert advisory. This is to be sent with a copy to the mediator.

b. Both parties should thereafter agree on the panel of experts who are well conversant with the issue under dispute.

c. The expert panel shall use its best endeavors to provide a neutral position on the issue.

d. If no resolution can be reached through the above means within 30 days then the matter should be referred to Arbitration.

(iv) Any dispute or difference whatsoever arising between the parties to this Agreement out of or relating to the construction, meaning, scope, operation or effect of this Agreement or the validity of the breach thereof shall be referred to a sole Arbitrator to be appointed by mutual consent of both the parties herein. If the parties cannot agree on the appointment of the Arbitrator within a period of one month from the notification by one party to the other of existence of such dispute, then the Arbitrator shall be appointed by the **High Court of Chhattisgarh**. The venue and seat of the Arbitration should specifically be laid down in the Agreement.

The provisions of the Arbitration and Conciliation Act, 1996 as amended from time to time will be applicable and the award made there under shall be final and binding upon the parties hereto, subject to legal remedies available under the law. Such differences shall be deemed to be a submission to arbitration under the Indian Arbitration and Conciliation (Amendment) Act 2015 or of any modifications, Rules or re-enactments thereof. The Arbitration proceedings (seat and venue) will be placed **at Raipur, Chhattisgarh**. Arbitration Proceedings shall be held in English & Hindi Language. Any legal dispute will come under the sole jurisdiction of the State jurisdiction of **Raipur, Chhattisgarh**.

17.30 Trademarks and Publicity

Neither Party may use the trademarks of the other Party without the prior written consent of the other Party except that Managed Service Provider may, upon completion, use the Project as a reference for credential purpose. Except as required by law or the rules and regulations of each stock exchange upon which the securities of one of the Parties is listed, neither Party shall publish or permit to be published either alone or in conjunction with any other person any press release, information, article, photograph, illustration or any other material of whatever kind relating to this Agreement, the service levels or the business of the Parties without prior reference to and approval in writing from the other Party. Such approval shall apply to each specific case and relate only to that case.

17.31 Data Ownership

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

17.32 Backup

The Managed Service Provider shall configure, schedule and manage backups of all the data including but not limited to files, folders, images, system state, databases and enterprise applications as per the policy defined by the Purchaser or MeitY.

17.33 Compliance with IS Security Policy

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

IN WITNESS WHEREOF the Parties have by duly authorized Representatives set their respective hands and seal on the date first above written in the presence of:

Witnesses Signed by

1. For and on behalf of Purchaser (FIRST PARTY)

2.

Name:

Designation:

Signature:

Seal:

1. For and on behalf of Managed Service Provider (SECOND PARTY)

2.

Name:

Designation:

Signature:

Seal:

17.34 Schedule I – Governance Schedule

Purpose

The purpose of this Governance Schedule is to:

a) establish and maintain the formal and informal processes for managing the relationship between the Purchaser and the Managed Service Provider
b) define the principles that both Parties wish to follow to ensure the delivery of the Services;
c) ensure the continued alignment of the interests of the Parties;
d) ensure that the relationship is maintained at the correct level within each Party;
e) create the flexibility to revise and maintain the relationship and this Agreement during the Term;
f) set out the procedure for escalating disagreements; and
g) enable contract administration and performance management.

Governance Structure

a) Project Managers: The relationship under this Agreement will be managed by the Project Managers appointed by each Party, who will provide the interface between the executive management of the respective Parties.
b) Project Governance Team (PGT) - Within 7 days following the Effective Date, Purchaser or its nominated agencies and the Managed Service Provider shall each appoint a Project Manager. In the event that either Party wishes to substitute its Project Manager it will do so in manner in which the original appointment is made and notify the other Party of such substitution as soon as reasonably practicable but at the latest within 7 days of the substitution.
c) The Project Managers shall have responsibility for maintaining the interface and communication between the Parties.
d) The PGT shall meet formally on a fortnightly / monthly / quarterly, as required, basis at a time and location to be agreed between them. These meetings will cover, as a minimum, the following agenda items: (i) consideration of periodic performance reports; (ii) consideration of matters arising out of the change control; (iii) escalated issues; (iv) matters to be brought before the PGT in accordance with this Agreement; (v) any matter brought before the PGT by the Managed Service Provider under this Agreement; and (vi) any other issue which either Party wishes to add to the agenda.

Governance Procedures

a) The Managed Service Provider shall document the agreed structures in a procedures manual.
b) The agenda for each meeting of the PGT shall be set to reflect the discussion items referred to above and extraordinary items may be added either with the agreement

of the Parties or at the request of either Party. Copies of the agenda for meetings of the PGT, along with relevant pre-reading material, shall be distributed at least one week in advance of the relevant meeting.

c) All meetings and proceedings will be documented. Such documents shall be distributed to the Parties and copies shall be kept as a record. All actions, responsibilities and accountabilities arising out of any meeting shall be tracked and managed.

d) The Parties shall ensure as far as reasonably practicable that the PGT shall resolve the issues and resolve the objectives placed before them and that members representing that Party are empowered to make relevant decisions or have easy access to empowered individuals for decisions to be made to achieve this.

e) In order to formally submit a Disputed Matter to the aforesaid for a resolution, one Party ("Claimant") shall give a written notice ("Dispute Notice") to the other Party. The Dispute Notice shall be accompanied by (a) a statement by the Claimant describing the Disputed Matter in reasonable detail and (b) documentation, if any, supporting the Claimant's position on the Disputed Matter.

f) The other Party ("Respondent") shall have the right to respond to the Dispute Notice within 7 days after receipt of the Dispute Notice. In the event that the parties are unable to resolve the Disputed Matter within a further period of 7 days, it shall refer the Disputed Matter to next level of the dispute resolution for action as per the process mentioned in Clause 1.26.

g) All negotiations, statements and / or documentation pursuant to these Articles shall be without prejudice and confidential (unless mutually agreed otherwise).

If the Disputed Matter is having a material effect on the operation of the Services (or any of them or part of them), the Parties will use all their respective reasonable endeavors to reduce the elapsed time in reaching a resolution of the Disputed Matter.

17.35 Schedule II – Change Control Schedule

This Schedule describes the procedure to be followed in the event of any proposed change to the Master Service Agreement (“MSA”), Project Execution Phase, SLA and Scope of Work. Such change shall include, but shall not be limited to, changes in the scope of services provided by the Managed Service Provider and changes to the terms of payment.

The Purchaser and Managed Service Provider recognize that change is an inevitable part of delivering services and that a significant element of this change can be accomplished by re-organizing processes and responsibilities without a material effect on the cost. The Managed Service Provider will endeavor, wherever reasonably practicable, to effect change without an increase in the terms of payment and Purchaser or its nominated agencies will work with the Managed Service Provider to ensure that all changes are discussed and managed in a constructive manner. This Change Control Schedule sets out the provisions which will apply to all the changes to this agreement.

Change Management Process

A. Change Control Note ("CCN")

(i) Change requests in respect of the MSA, the Project Execution, the operation, the SLA or Scope of work will emanate from the Parties' respective Project Manager who will be responsible for obtaining approval for the change and who will act as its sponsor throughout the Change Control Process and will complete Part A of the CCN attached as

Annexure A hereto. CCNs will be presented to the other Party's Project Manager who will acknowledge receipt by signature of the CCN.

(ii) The Managed Service Provider and the Purchaser or its nominated agencies, during the Project Execution Phase and the Purchaser or its nominated agencies during the Operations and Management Phase and while preparing the CCN, shall consider the change in the context of the following parameter, namely whether the change is beyond the scope of Services including ancillary and concomitant services required and is suggested and applicable.

(iii) It is hereby also clarified here that any change of control suggested beyond 25 % of the value of this Project will be beyond the scope of the change control process and will be considered as the subject matter for a separate bid process and a separate contract. It is hereby clarified that the 25% of the value of the Project as stated in herein above is calculated on the basis of bid value submitted by the Managed Service Provider and accepted by the Purchaser or its nominated agencies or as decided and approved by Purchaser or it Nominated Agencies. For arriving at the cost / rate for change up to 25% of the project value, the rates submitted in the Financial Proposal shall be considered.

B. Quotation

(i) The Managed Service Provider shall assess the CCN and complete Part B of the CC. In completing the Part B of the CCN, the Managed Service Provider shall provide as a minimum:

a) a description of the change
b) a list of deliverables required for executing the change;
c) a time table for execution;
d) an estimate of any proposed change
e) any relevant acceptance criteria
f) an assessment of the value of the proposed change;
g) material evidence to prove that the proposed change is not already covered within the Agreement and the scope of work

(ii) Prior to submission of the completed CCN to the Purchaser, or its nominated agencies, the Managed Service Provider will undertake its own internal review of the proposal and obtain all necessary internal approvals. As a part of this internal review process, the Managed Service Provider shall consider the materiality of the proposed change in the context of the MSA and the Project Execution affected by the change and the total effect that may arise from execution of the change.

C. Costs

Each Party shall be responsible for its own costs incurred in the quotation, preparation of CCNs and in the completion of its obligations described in this process provided the

Managed Service Provider meets the obligations as set in the CCN. In the event the Managed Service Provider is unable to meet the obligations as defined in the CCN then the cost of getting it done by third party will be borne by the Managed Service Provider.

D. Obligations

The Managed Service Provider shall be obliged to execute any proposed changes once approval in accordance with above provisions has been given, with effect from the date agreed for execution and within an agreed timeframe. The Managed Service Provider will not be obligated to work on a change until the parties agree in writing upon its scope, price and/or schedule impact. The cost associated with any service/software/hardware/licenses should not exceed the price quoted in the Managed Service Provider's proposal.

17.36 ANNEXURE

17.36.1 ANNEXURE A - Format for Change Control Notice

Change Control Note	**CCN Number:**
Part A: Initiation	
Title:	
Originator:	
Sponsor:	
Date of Initiation:	
Details of Proposed Change	
(To include reason for change and appropriate details/specifications. Identify any attachments as A1, A2, and A3 etc.)	
Authorized by Purchaser	Date:
Name:	
Signature: Received by the IA	Date:
Name:	
Signature:	
Change Control Note	**CCN Number:**
Part B : Evaluation	

(Identify any attachments as B1, B2, and B3 etc.) Changes to Services, charging structure, payment profile, documentation, training, service levels and component working arrangements and any other contractual issue.
Brief Description of Solution:
Impact:
Deliverables:

Timetable:	
Charges for Implementation: (including a schedule of payments)	
Other Relevant Information: (including value-added and acceptance criteria)	
Authorised by the Implementation Agency	**Date:**
Name:	
Signature:	

Change Control Note	**CCN Number :**
Part C : Authority to Proceed	
Implementation of this CCN as submitted in Part A, in accordance with Part B is: (tick as appropriate)	
Approved	

Rejected **Requires Further Information** (as follows, or as Attachment 1 etc.)	

For DTAP	**For the Implementation Agency**
Signature	Signature
Name	Name
Title	Title
Date	Date

17.36.2 ANNEXURE B – Scope of Work to be delivered by MSP

<<The entire Scope of Work– *To be filled upon finalization of the successful bidder.****>>***

17.36.3 ANNEXURE C – Technical Compliance

<< Bid Proposal submitted by MSP. The Bid proposal shall include all the documents submitted by successful bidder as part of technical complaince - To be filled up after the finalization of the bidder>>

17.36.4 ANNEXURE D – Bill of Material (with Cost break-up)

1. Detailed Bill of Materials (along with technical specifications) with Complete Break-up of Costs and Pricing for Different Items as submitted by successful bidder as part of commercial proposal

<<To be filled up after the finalization of the bidder>>

18. Non-Disclosure Agreement

This Non-Disclosure Agreement ("Agreement") is made and entered into **____ day of …………., 2023** at _________________, India.

BETWEEN

Director of Treasury, Accounts & Pension (DTAP), Finance Department, Government of Chhattisgarh having its office at ______________________________________(hereinafter referred to as 'DTAP')

AND

…………………….., having its office at _______________________________ (hereinafter referred to as 'MSP')

Each of the parties mentioned above are collectively referred to as the '***Parties***' and individually as a '***Party***'.

WHEREAS:

1. Purchaser is desirous to implement the project of -----------------------.
2. The Purchaser and Implementation Agency have entered into a Master Services Agreement dated <***> (the "***MSA***") as well as a Service Level Agreement dated <***> (the "***SLA***") in furtherance of the Project.
3. Whereas in pursuing the Project (the "***Business Purpose***"), a Party ("Disclosing Party) recognizes that they will disclose certain Confidential Information (*as defined hereinafter*) to the other Party ("Receiving Party").
4. Whereas such Confidential Information (*as defined hereinafter*) belongs to Receiving Party as the case may be and is being transferred to the Disclosing Party to be used only for the Business Purpose and hence there is a need to protect such information from unauthorized use and disclosure.

NOW, THEREFORE, in consideration of the foregoing and the covenants and agreements contained herein and, in the Contract, the parties agree as follows:

1. **Definitions.** As used herein:

(a) The term "Confidential Information" shall include, without limitation, all information and materials, furnished by DTAP to MSP in connection with corporates/citizen/users/persons/customers data, products and/or services, including information transmitted in writing, orally, visually, (e.g. video terminal display) or on magnetic or optical media, and including all proprietary information, customer & prospect lists, trade secrets, trade names or proposed trade names, methods and procedures of operation, commercial or marketing plans, licensed document know-how, ideas, concepts, designs, drawings, flow charts, diagrams, quality manuals, checklists, guidelines, processes, formulae, source code materials, specifications, programs, software packages, codes and other intellectual property relating to the DTAP's data, computer database, products and/or services. Confidential Information shall also include results of any tests, sample surveys, analytics, data mining exercises or usages etc. carried out by MSP in connection with the DTAP's or any government department's information including citizen/users/persons/customers personal or sensitive personal information as defined under any law for the time being in force.

(b) The term, “DTAP” shall include the officers, employees, agents, consultants, other applicable agencies and representatives of DTAP and its assigns and successors.

(c) The term, “MSP” shall include the directors, officers, employees, agents, consultants, other applicable agencies and representatives of MSP, including its applicable affiliates, subsidiary companies and permitted assigns and successors.

2. **Protection of Confidential Information.** With respect to any Confidential Information disclosed to MSP or to which MSP has access, MSP agrees that it shall:

(a) Use the Confidential Information only for accomplishment of the services to be performed under the Contract and in accordance with the terms and conditions contained herein;

(b) Maintain the Confidential Information in strict confidence and take all reasonable steps to enforce the confidentiality obligations imposed hereunder, but in no event takes less care than it takes to protect the confidentiality of its own proprietary and confidential information and that of its clients;

(c) Not make or retain copy of any Confidential Information DTAP except as necessary, under prior written permission from DTAP, in connection with the services to be performed under the Contract, and ensure that any such copy is immediately returned to DTAP even without express demand from DTAP to do so;

(d) Not disclose or in any way assist or permit the disclosure of any Confidential Information to any person or entity without the express written consent of DTAP except as provided in clause 6 below; and

(e) Return to DTAP, or destroy, at DTAP’s direction, any and all Confidential Information disclosed in a printed form or other permanent record, or in any other tangible form (including without limitation, all copies, notes, extracts, analyses, studies, summaries, records and reproductions thereof) immediately upon the earlier to occur of:

(i) expiration or termination of the Contract,
or

(ii) on request of DTAP.

(f) Not discuss with any member of public, media, press or any other person about the nature of arrangement entered between DTAP and MSP or the nature of services to be provided by the MSP to the DTAP.

3. **Onus.** MSP shall have the burden of proving that any disclosure or use inconsistent with the terms and conditions hereof falls within any of the exceptions provided in clause 4 below.

4. **Exceptions.** The obligations of confidentiality as mentioned in this Agreement shall not apply to any information:

(a) Which has become generally available to the public without breach of this Agreement by MSP; or

(b) Which at the time of disclosure to MSP was known to MSP free of confidentiality restriction as evidenced by documentation in MSP’s possession; or

(c) Which DTAP agrees in writing is free of such confidentiality restrictions

(d) Is required to be disclosed by law, regulation or Court Order, provided that the recipient gives prompt written notice to the discloser of such legal and regulatory requirement to disclose so as to allow the discloser reasonable opportunity to contest such disclosure.

5. **Remedies.** MSP acknowledges and agrees that (a) any actual or threatened unauthorized disclosure or use of the Confidential Information by MSP would be a breach of this Agreement and may cause immediate and irreparable harm to DTAP; (b) MSP damages from such unauthorized disclosure or use may be impossible to measure accurately and injury sustained by DTAP may be impossible to calculate and remedy fully. MSP acknowledges that in the event of such a breach, DTAP shall be entitled to specific performance by

   MSP of MSP's obligations contained in this Agreement. MSP shall indemnify, save, hold harmless and defend DTAP promptly upon demand and at its expense, any time and from time to time, from and against any and all suits, proceedings, actions, demands, losses, claims, damages, liabilities, costs (including reasonable attorney's fees and disbursements) and expenses (collectively, "Losses") to which DTAP may become subject, in so far as such Losses arise out of, in any way relate to, or result from breach of obligations under this Agreement

6. **Need to Know**. MSP shall restrict disclosure of Confidential Information to its employees and/or consultants who have a need to know such information for accomplishment of services under the Contract provided such employees and/or consultants have agreed to abide by the terms and conditions of this Agreement and agree that they shall not disclose such Confidential Information to any affiliates, subsidiaries, associates and/or third party without prior written approval of DTAP.

7. **Intellectual Property Rights Protection.** No license to MSP, under any trademark, patent, copyright, design right, mask work protection right, or any other intellectual property right is either granted or implied by the conveying of Confidential Information to MSP.

8. **No Conflict**. The parties represent and warrant that the performance of their obligations hereunder do not and shall not conflict with any other agreement or obligation of the respective parties to which they are a party or by which the respective parties are bound.

9. **Authority.** The parties represent and warrant that they have all necessary authority and power to enter into this Agreement and perform their obligations hereunder.

10. **Governing Law.** This Agreement shall be interpreted in accordance with and governed by the substantive and procedural laws of India and the parties hereby consent to submit to the exclusive jurisdiction of Courts and/or Forums situated at Raipur/Bilaspur, Chhattisgarh.

11. **Entire Agreement.** This Agreement constitutes the entire understanding and agreement of the parties, and supersedes all previous or contemporaneous agreement or communications, both oral and written, representations and under standings among the parties with respect to the subject matter hereof.

12. **Amendments.** No amendment, modification and/or discharge of this Agreement shall be valid or binding on the parties unless made in writing and signed on behalf of each of the parties by their respective duly authorized officers or representatives.

13. **Binding Agreement.** This Agreement shall be binding upon and inure to the benefit of the parties hereto and their respective successors and permitted assigns.

14. **Severability.** It is the intent of the parties that in case any one or more of the provisions contained in this Agreement shall be held to be invalid or unenforceable in any respect, such provision shall be modified to the extent necessary to render it, as modified, valid and enforceable under applicable laws, and such invalidity or unenforceability shall not affect the other provisions of this Agreement.

15. **Waiver.** If either party should waive any breach of any provision of this Agreement, it shall not thereby be deemed to have waived any preceding or succeeding breach of the same or any other provision hereof.

16. **Survival.**MSP agrees that all of their obligations undertaken herein with respect to Confidential Information received pursuant to this Agreement and obligations of indemnity shall survive for a period of 5 years after any expiration or termination of the Contract.

17. **Non-solicitation.** During the term of this Agreement and thereafter for a further period of two (2) years MSP shall not solicit or attempt to solicit DTAP's employees and/or consultants, for the purpose of hiring/contract or to proceed to conduct operations/business similar to DTAP with any employee and/or consultant of the DTAP who has knowledge of the Confidential Information, without the prior written consent of DTAP. This section will survive irrespective of the fact whether there exists a commercial relationship between MSP and DTAP.

18. **Term.** This Agreement shall come into force on the date first written above and, subject to aforesaid clause 16, shall remain valid up to expiry or termination of the Contract.

IN WITNESS HEREOF, and intending to be legally bound, the parties have executed this Agreement to make it effective from the date and year first written above.

For DTAP……….,	For ……………………
Name:	Name: ………………
Title:………………………	Title: …………….
WITNESSES:	WITNESSES:
1.	2.

--------------------------- End of Document-----------------------