Request for Expression of Interest (EOI) for the procurement of Cloud Services for Finance Data Center, Uttarakhand

Department of Finance

Government of Uttarakhand

Directorate of Treasuries, Pension & Entitlements, Uttarakhand

23, Laxmi Road, Dalanwala, Dehradun

Uttarakhand – 248001

Tel: 0135- 2226852, 2226860

E-mail- treas-dir-uk@nic.in, treas-ua@nic.in

DIRECTORATE OF TREASURIES, PENSION & ENTITLEMENT, UTTARAKHAND, 23, LAXMI ROAD, DALANWALA, DEHRADUN – 248001

Letter No.15045/FDC/DTPE/CLOUD/2022 Dated 06 Feb, 2023

(Expression Of Interest Notice)

The Directorate of Treasuries, Pension & Entitlements, Uttarakhand is seeking expressions of interest for the procurement of Cloud Services from MeitY-empaneled Cloud Service Providers (CSPs)/Managed Service Providers (MSPs)/SI for the Finance Data Center of the state.

The Expression of Interest document, which includes the scope of work, can be downloaded from the websites **https://uktenders.gov.in/** and **https://ekosh.uk.gov.in/** starting on **February 07, 2023 at 11:00 AM**. Interested bidders must submit their proposals by **February 24, 2023 at 3:00 PM**. For any queries, interested parties can contact the department at **treas-ua@nic.in.**

Director,
Directorate of Treasuries, Pension and Entitlements
Dehradun, Uttarakhand

Key Details

S. No	Milestone	Date and time
1	EOI Reference Number	15045
2	Name of work	Procurement of Cloud Services for Finance Data Center, Uttarakhand
3	Place of availability of EOI Document	https://uktenders.gov.in/ and https://ekosh.uk.gov.in/
4	Date of publication of EOI notice	07th February, 2023 11:00Hours
5	Pre-Bid Meeting	13th Feb, 2023 12:00 Hours
6	Last date for submission of EOI	24thFebruary,2023 15:00 Hours
7	Opening of EOI	24thFebruary,2023 16:00 Hours
8	Evaluation of EOI proposals	27thFebruary,2023 11:00 Hours
9	Presentation by the participants	06th March to 10th March, 2023 12:00 Hours
10	Address for communication	Director, Directorate of Treasuries, Pension & Entitlements, 23 Laxmi Road, Dalanwala, Dehradun, Uttarakhand
11	Email ID	treas-ua@nic.in

Table of Contents

Contents

Note- Term "Bidder" in this EoI refers CSP/MSP/SI

Glossary of Terms

Acronym	Expansion
CSP	Cloud Service Provider
DTPE	Directorate of Treasuries, Pension & Entitlements
EOI	Expression of Interest
EMD	Earnest Money Deposit
EMI	Equated Monthly Installment
EQI	Equated Quarterly Installment
FDC	Finance Data Center
GI Cloud	Government of India Cloud
GCC	Government Community Cloud
IFMS	Integrated Financial Management System
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
IOPS	Input/output operations per second
MSP	Managed Service Provider
MeitY	Ministry of Electronics and Information Technology
O&M	Operations and Maintenance
PaaS	Platform as a Service
PCI DSS	Payment Card Industry Data Security Standard
RAC	Real Application Cluster
RPO	Recovery Point Objective
RTO	Recovery Time objective
SAS	Serial Attached SCSI
SATA	Serial Advanced Technology Attachment
SCSI	Small Computer System Interface
SDC	State Data Center
SI	System Integrator
SLA	Service Level Agreement
SSD	Solid State Drive
VLAN	Virtual Local Area Network
VLB	Virtual Load Balancer
VM	Virtual Machines

1. Project Background

Directorate of Treasuries, Pension & Entitlements (DTPE) is a department of the State Government that operates under the Ministry of Finance, Uttarakhand. The department is responsible for managing all financial transactions made by the State Government through the Integrated Financial Management System (IFMS). The IFMS is run by the Finance Data Center (FDC) and is overseen by the DTPE. The department's main responsibilities include reviewing bills submitted by various departments for payment, finalizing payments, and maintaining data of over 4600 DDOs, 109 HODs, 1.4 Lakh employees, 1.6 Lakh pensioners, and more than 3 Lakh vendors. The DTPE uses Integrated Financial Management System (IFMS) to manage this data and make it available on the web with a single click.

IFMS includes two applications: one for government departments (IFMS 1.0) and one for treasuries (IFMS 2.0). IFMS 1.0 is accessible on the internet, while IFMS 2.0 is only available on the state SWAN and is not exposed to the internet. The IFMS uses Oracle 12c (Enterprise edition) as its database and is hosted at the Finance Data Center in Dehradun. The IFMS application has the following main modules:

Sl. No.	Module	Sl. No.	Module
1	Pay Roll	13	DDO
2	Claims	14	e-Challan
3	Pension Disbursement	15	Chits, Firms and Societies
4	E-Payment	16	Pension sanction
5	HRMS	17	SGHS
6	Works Accounting	18	Taxation
7	PLA	19	NPS
8	Receipt Accounting	20	Budget Disbursement
9	Payment Accounting	21	Budget Maintenance
10	GIS	22	PFMS
11	GPF	23	AG Module
12	Virtual Treasury	24	Generic Modules

IFMS also has integration with different institutions as given below:

Sl. No.	Department/Agency	Sl. No.	Department/Agency
1	Reserve Bank of India (RBI)	12	Excise Department
2	State Bank of India (SBI)	13	Transport department
3	Goods and Services Network (GSTN)	14	Directorate of Industries
4	NSDL	15	Police Department
5	Public Financial Management System (PFMS)	16	Planning Department
6	C-DAC	17	National Scholarship Portal
7	Jeevan Pramaan	18	PASARA
8	NIC - SMS Gateway	19	Apuni Sarkar
9	NIC - Email gateway	20	NPCI
10	Stock Holding Corporation of India Ltd	21	Digi locker
11	Social Welfare Department	22	State Tax Department

IFMS has several key stakeholders including the Accountant General, various government departments, PFMS, RBI, and agency banks, among others. The government has plans to transition to a paperless system starting April 1, 2023. Additionally, the government also intends to incorporate Aadhaar Authentication for user verification in future. For information about the current setup, please refer to **Table-3.**

2. Purpose of the EOI

The objective of this Expression of Interest (EOI) is to allow the Directorate of Treasuries, Pension & Entitlements (DTPE) to acquire cloud services from a MeitY empaneled Cloud Service Providers (CSPs)/Managed Service Providers (MSPs) for hosting the Integrated Financial Management System (IFMS) software. This is in line with the Cloud First policy of MeitY (As a part of the MeghRaj initiative, MeitY came out with the 'Cloud First' policy under which all the departments are required to assess and adopt cloud computing for their current as well as new applications). The EOI also outlines the key responsibilities of the DTPE and the Meity-empaneled CSP/MSP during the procurement of cloud services.

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

Production,
Development/Testing,
Staging, and
Disaster Recovery.

The Directorate of Treasuries, Pension & Entitlements (DTPE) also hopes to achieve cost savings through an "OpEx"/ "pay-per-use" model, where DTPE only pays for the resources, it uses. The Expression of Interest (EOI) must be submitted online through https://uktenders.gov.in/

3. EOI Issuing Authority

This EOI is issued by DTPE to the bidders and is intended to procure cloud services.

S. No.	Item	Description
	Project Title	**Procurement of Cloud Services for Finance Data Center**
	Project Initiator /EOI Issuer Details	
1	Department	Directorate of Treasuries, Pension & Entitlements
2	Contact Person	Jagat Singh Chauhan, Additional Director 0135-2226804
3	Contact Person	Manoj Kumar Pandey, Deputy Director 0135-2226852
4	Email Address for all Bid Correspondence	treas-ua@nic.in
5	Estimated Value of the Project	Rs. 3.50 Crore (Rupees Three Crore Fifty Lakh only) per year
6	Address for the purpose of Bid Submission	23 Laxmi Road, Dalanwala, Dehradun, Uttarakhand-248001
7	Website	https://ekosh.uk.gov.in/, https://ifms.uk.gov.in/

4. Scope of Work

Directorate of Treasuries, Pension and Entitlements, Uttarakhand wishes to engage a MeitY empaneled Cloud Service Provider/Managed Service Provider for providing Cloud Services for hosting the IFMS applications for a period of 3 years, with the possibility of an extension for another 2 years upon completion of the third year, at the discretion of the DTPE.

The selected bidder will be responsible to fulfil 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 would be responsible for providing cloud for setting up, installation, configuration, management, up gradation, 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 empaneled 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 CSP 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 CSP 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 IFMS application and database in the cloud. The proposed deployment plan for the IFMS application includes:
    a. Production
    b. Development/Testing
    c. Staging
    d. Disaster Recovery
3. **Support Finance Data Center (FDC):** The Bidder will support Finance Data Center (FDC)for implementation, management and monitoring of IFMS software in cloud environment. DDOS, IPS, IDS Services, anti-malware, vulnerability scanning and penetration testing etc to be configured for IFMS application and ensure 99.9 % uptime of cloud services as per agreement. Bidder will also be responsible for providing 24x7x365 support to FDC in case of any issues related to the cloud services and connectivity.
4. **Connectivity:** The bidder shall ensure dedicated leased line connectivity with redundancy of 1 Gbps with necessary equipment from the Data center of CSP to State Data Center, Uttarakhand for uploading or migrating database/files and day to day operations and maintenance of IFMS software etc. The bidder should also propose CSP's own IP addresses for DC/DR and have multiple upstream providers so that if connectivity from either service provider goes down, redundancy is maintained. Offered cloud service shall allow FDC users to securely and remotely, load applications and data onto the computing or virtual machine instance from the SSL VPN clients only as against the public internet.
5. **Migration of applications and databases:** The Bidder will be responsible for migrating to cloud in co-ordination with the FDC 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 FDC. 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.

DB should support minimum 20,000 IOPS with more than 900 Mega Bytes Per Second (MBPS) throughput for a 500 GB storage volume

3- BYOL mode must be Available.

Note: The DB Storage Should be SSD with very high IOPS and must be shared (R/W) across DB Nodes as Oracle DB has to be Deployed in Cluster, Oracle RAC/Equivalent Active Active solution.

4- 1 Physical Core = 2 vCPU

5- DB-Software= Compatible with the existing database in HA.

6- OS Required = Linux 7.X or Later , Microsoft Windows Server 2019 Standard or Later

7- Normally DR would Run with 25% of DC Configuration and would be on Standby Except Database and App Server. In case of Switchover or Failover DR should be running with Full 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.

8- App Server and Integration Server in DC and DR should be in Sync.

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.

RPO Should be Zero and RTO Should be 30 Minutes

6. **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.

7. **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.

8. **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 bidder must provide 1 Gbps leased line with different ISPs in a High Availability (HA) configuration terminating at the State Data Centre, ITDA, IT Park Shastradhara Road, Dehradun, Uttarakhand.

p) 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.

9. **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.

10. **Root Access:** The bidder will be responsible to provide the access of root account of proposed CSP to Finance Data Center (FDC).

11. **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 as per specifications provided below:

a) CSP 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 zero minutes and RTO shall be less than or equal to 0.5 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 FDC jointly. Certificate for DR drill should be submitted to FDC 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 FDC 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.

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.

12. **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 DTPE.

13. **Interoperability support:** Bidder shall provide inter-operability support with regard to APIs and Data Portability.
14. **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 DTPE promptly in the event of security incidents or intrusions, or any request to access data, to enable DTPE 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.
15. **Documentation:** Bidder shall provide necessary technical documentations, design documentations, standard Operating Procedures (SOPs) required for operations and management of services.
16. **Risk management**: All risk management related to migration; migration plan shall be worked out with FDC.
17. **Assessment of future needs:** The bidder shall asses the future needs of IFMS application in coordination with FDC.
18. **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.
19. **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.
20. **DR Drills:** Bidder shall be responsible for conducting business continuity/DR drills. Bidder has to follow Standard Operating Procedures (SOP) and inform Finance Data Center (FDC) in advance for such drills which will have to be conducted four times a year, with 15 days' prior notice.
21. **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.
22. **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.
23. **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.
24. **Compliance:** The environment of Cloud shall comply with the respective empanelment

compliance requirements published by Ministry of Electronics Information and Technology, Government of India.

25. **Malware Websites:** The Provider must provide Proactive and Request based takedown of Phishing, Malware websites, Fake Social Media Accounts, Mobile Applications, Advertisements etc
26. **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.
27. **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,

    ▪ The Purchaser should be able to set percentage / quantity of RAM consumption to trigger new virtual machines.

    ▪ The Purchaser should be able to set percentage / quantity of network bandwidth to trigger new virtual infrastructure.

    k) 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.

    l) 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.
28. **Training:** Selected Bidder should provide cloud training/certification to DTPE nominated officials/personnel on usage of the Console and any other technical aspect for monitoring of IFMS project in cloud. The Bidder will also train and transfer the knowledge to the replacement agency or Finance Data Center (FDC) to ensure continuity and performance of services post expiry of Contract. Additionally, the bidder must provide training and certification for the FDC Team on Cloud Operations, network, security, Database, Application Performance Management (APM), Log Analytics, General Analytics Services, Active Directory Services, and WSUS Services in cloud
29. **Manpower:** Bidder shall provide minimum 2 Cloud engineers/cloud professionals offsite throughout the contract period to support FDC.
30. **Bidders must note that:**

    The Uttarakhand Treasury department 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 DTPE 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 fail-over/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. DTPE 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 DTPE.
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. Bidder should ensure to protect the workload hosted in cloud with Antimalware, HIPS, Firewall, Application control, FIM, Log correlation, C&C prevention and Recommendation Scan must be available in single agent supporting Windows, Linux RedHat, CentOS, Oracle, Debian, SUSE, Ubuntu, Solaris, AIX, Amazon Linux OS platforms having management console on Window and RHEL.
10. Bidders should propose solution having capability to automatically recommend rules for host-based Intrusion prevention, integrity Monitoring & log analysis module as per the Server OS which can be scheduled for automatic provisioning & De-provisioning of rules when not required also customized rule creation should support pattern matching like Regular Expressions, simpler String Patterns and the rule will be triggered on a match.
11. Bidder should provide solution having capability to provide the virtual patch against the known and zero-day vulnerabilities, which should be automatically update as in when the vulnerability is discovered using the automatic recommendation feature.
12. Proposed solution should have the capability to protect the running container at runtime from intrusion and malware
13. The solution should be deployed as a minimal agent on the cloud workloads such as VMs, Containers and Serverless to provide asked security features to the workloads and a should provide a unified workload protection framework to protect cloud native applications across

different environments such as cloud managed Kubernetes platform, self-operated Kubernetes platform, OpenShift and etc.

14. Bidder should incorporate the capability to maintain the security posture of cloud environment which can integrate over API with multiple accounts. and multiple regions of in public cloud environment such as AWS, Azure and GCP with a single centralized console and generate improper network activity, misconfiguration, compliance related and anomalous activity alerts, should continuously discover and automatically classify cloud resources as soon as they are deployed.
15. Bidders should ensure to incorporate capability to continuously monitor all cloud resources for misconfigurations and provide out-of-box policies to check for security best practices for IaaS and PaaS configuration. Should provide ability to clone, customize, and run an existing policy, should have ability to enforce policy governance guardrails that can automatically trigger alerts for misconfigurations and configuration drift. It should have the ability to provide guided remediation details for issues detected out-of-the-box, Ability to auto-remediate infrastructure changes based on a specific policy requirement with custom action and should have the capability to support the custom workflow auto-remediation for the critical use cases.
16. The solution should have the ability to report on compliance status for cloud infrastructure services as per: minimum compliance reporting for PCI DSS, CIS (AWS, Azure, GCP), SOC 2, NIST 800-53 Rev5, ISO 27001 etc. Also should have option & ability to create custom compliance templates based on business requirements. Additional solution should have the capability to share the misconfiguration details with centralized detection and response solution which should support the log correlation of cloud misconfiguration along with the other workload and network assets on cloud.
17. The solution should have the capability to scan the containerized images at registry and post build against the vulnerabilities, Malware, hardcoded secret and compliance violation at each layer of container image. It should also provide the runtime container security against security drift defined in MITRE ATTACK framework and should have the capability to allow only secure hardened images into the cluster. Additionally, solution should provide the maximum coverage in finding the zero-day vulnerability in open source, third party etc. Solution provider should be contributing at least 30 zero-day/Undisclosed vulnerabilities to Microsoft continuously from past 5 years and data should be publicly available also vulnerability research data will require third party validation from agencies such as Omdia for highest vulnerabilities contribution.
18. The bidder should provide a IPS solution to protect the cloud assets from intrusion attack at perimeter level. IPS solution should be dedicated purpose-built solution, NOT a part of Firewall module or UTM solution. The solution must provide Layer 7: Application protection to protect workloads against known and unknown threats brute force attacks, shellshock, Log4J type vulnerability exploits etc also should be able to deploy in a multi cloud environment and should support cloud native infrastructure capabilities while deploying.
19. IPS Should support VA scanners (Qualys, Rapid 7, Nessus) to fine tune the IPS policy and The IPS filter must support network action set such as Block (drop packet), Block (TCP Reset), Permit, Trust, Notify, Trace (Packet Capture), Rate Limit and Quarantine & proposed IPS solution must support signatures, protocol anomaly, vulnerabilities and traffic anomaly filtering methods to detect attacks and malicious traffic.
20. The solution should be deployed as a virtual appliance rather than physical appliance and if

required should be available as in OEM managed infrastructure. It should support the inspection capability between different Virtual private network as well as should be capable of inspecting the traffic coming from Internet. The solution should also support minimum throughput of 10 Gbps with autoscaling and self-healing capabilities. Solution must be a custom built on premise dedicated solution and should not be from NGFW, Routing, Switching, Load Balancer based vendor to avoid single point of failure adhering NCIIPC, Cert-In, NIST and DSCI guidelines.

21. The bidder should have the solution which should be capable of scanning the data uploaded or stored in object storages against the malware and should also support multiple file type including .BIN, .EXE, .MP4, .PDF, .TXT, .ZIP and more.

22. The object storage scanning solution should support cloud native infrastructure and architecture. Solution should be deployed at object storage level to scan the files whenever uploaded against malware. The solution should work in local cloud environment and the respective solution should not share the data outside India border i.e., solution should have local India data center.

23. The bidder is expected to propose a solution for setting up a cloud infrastructure that aligns with the existing setup of the FDC as detailed in Table-3.

5. Eligibility Criteria and evaluation process of EOI proposal

The bidder must comply with eligibility criteria listed below and submit the required documents in the proper format as specified in Table 8 of Annexure IV in order to qualify for the next stage of the bidding process.

A. General conditions

a. Bidder means MSP/SI/CSP.
b. MSP/SI refers to a single entity participating in the consortium as a partner along with the CSP. Both entities shall be referred to as Consortium Partners. The Lead bidder must provide a declaration in the Consortium Agreement
c. If the CSP participates in the bid as a single entity, it will be responsible for fulfilling all of the conditions outlined in the eligibility criteria.

Table 1

S. No.	Requirements	Applicability	Evidence to be submitted~
1.	Bidder must be a Legal Entity i.e. 1) A company incorporated under the Indian Companies Act, 2013 or any other previous company law as per section 2 (20) of the Indian Companies Act 2013 on or before 01-04-2017 2) Registered with the Income Tax (PAN) and GST (GSTN)Authorities in India with active status	Lead Bidder/Bidder	Certified by Authorized Signatory: 1. Copy of Certificate of Incorporation/Registration 2. Copy of Registration Certificates with the GST & IT (PAN)Authorities

S. No.	Requirements	Applicability	Evidence to be submitted~
2.	The cloud services offered by the Bidder should provide Meity empanelment certificate for the Cloud Service Provider(CSP).	CSP	Valid certificate from Meity.
3.	Bidder should provide undertaking from CSP regarding authorization for providing cloud & security services.	Lead Bidder/Bidder	Undertaking from CSP. MAF of CSP and Security Services.
4.	The Bidder should have average annual turnover of at least INR 10 Crore from Cloud (CSP) and Data Centre Infrastructure services (i.e. FY2019-20, FY20-21 and FY2021-22)	Lead Bidder/ Bidder	CA Certified copy should be provided mentioning business from the Cloud service and Data Centre Infrastructure services.
5.	The bidder should have positive Net worth in last 3 financial years (i.e. FY2019-20, FY20-21andFY2021-22)	Lead Bidder/ Bidder	Chartered Accountant certificate for Net-worth of the company. Copy of the audited profit and loss account of the company showing turnover of the company for last three years.
6.	The Bidder should not have been blacklisted or conflict of activities by any State Government, Central Government or any other Public Sector undertaking or a corporation or any other Autonomous Organization of Central or State Government for breach of Contractual Conditions as on bid submission date.	Lead Bidder, Consortium Partner, CSP	Self-declaration from Bidder
7.	The CSP should provide the following Cloud Security Certificates of proposed cloud service ❖ ISO27017/27018 ❖ ISO27701 ❖ ISO22301 ❖ Tier-3certification	CSP	Submit valid Copy of the Certificates at the time of bid submission.
8.	The bidder should provide the cloud service having accreditation relevant to security, availability, confidentiality, processing, integrity and privacy trust services principles SOC1, SOC2/SOC3, PCIDSS	CSP	Third Party Audited/Applicable reports to be submitted
9.	The Bidder should have annual turnover of INR 50Cr. For last 3 financial years (i.e. FY2019-20, FY20-21and FY2021-22)	Lead Bidder/ Bidder	CA Certificate and certified copy of turnover to be submitted

S. No.	Requirements	Applicability	Evidence to be submitted~
10.	The bidder must have on its roll at least 5 technically Cloud Certified professionals and prior experience in providing the Cloud/ Data Centre Infrastructure services as on 31-03- 22	Lead Bidder/Consortium Partner/Bidder	a) Certificate from bidders HR Department for number of Technically qualified professionals employed by the company. b) Details of the employees to be deployed along with certified copies of Cloud certifications done.
11.	Bidder/CSP should have Completed at least one project of cloud services/Data Center Infrastructure Services with similar nature involving hosting of financial application and database in cloud environment to any Government Organization /PSU with project cost worth more than 3.5 crore.	Lead Bidder/Consortium Partner/Bidder	Copy of work order Copy of Commissioning certificate/Completion certificate

B. Minimum Technical Specification/ Special Conditions:

Following are the mandatory compliance need to be submitted by the bidder in their technical proposal on Cloud environment: -

Table2

Infrastructure as a Service (IaaS)– Compute – Virtual Machine			
S.No	**Description**	**Compliance (Yes/No)**	**Page No.**
1	CSP shall support industry Oracle Linux and windows OS.		
2	The CSP should ensure that underlying processors should not have been discontinued by the processor OEM at time of bidding and they are the latest generation of Processors.		
3	Auto scaling (Up & Down) of compute based on metrics (CPU, Memory, Storage) & time/schedule based to align with business demand like month end peak, quarterly & annual peaks.		
4	Database required is Oracle Enterprise Edition with Clustering to support Active-Active deployment to achieve high availability at database layer. It should be supported by OEM of database. It should support BYOL method.		
5	Cloud should have capability of Automatic and manual back-ups to support point in time recovery.		
6	Cloud should support full encryption of entire database, backups and all network connections. In addition, should provide Database auditing in terms of Login failures, Modifications to user accounts or database structures.		

7	Proposed Data Center and Disaster Recovery should be in two different seismic zones.		
8	CSP should support copying snapshots of any size between different regions for disaster recovery purposes		
9	Cloud should provide built-In Machine Learning Library like Clustering, Classification, Regression, Feature Extraction, Text Mining Support, Statistical Functions etc.		

DTPE reserve the right to validate the claims made in the eligibility criteria by the bidder during the technical evaluation and may further disqualify based on the findings. Sub-contracting is not allowed.

6. Existing Setup

Table-3- Existing setup

Currently the whole Infrastructure is deployed at Finance Data Center (DC) and DR at SDC, ITDA. AT DC We are Using Rack Servers and Blade Servers for Deployment of Database, Application, and Integrations. we are using San Storage of HP 3PAR of around 50 TB Space. Below is the Summarized View of the Infrastructure:

Serial No.	Server	Cores	RAM	Storage
1	DB-Server-Node-1	16	512 GB	8 TB
2	DB-Server-Node-2	16	512 GB	
3	App-Server-1	16	256 GB	1 TB
4	App-Server-2	16	256 GB	1 TB
5	App-Server-3	8	64 GB	500 GB
6	Domain-Server	16	256 GB	1 TB
7	Virtualization-Server	16	256 GB	1 TB
8	Integration-Server	16	256 GB	500 GB
9	Sftp-Server-1 (VM)	8	64 GB	300 GB
10	Sftp-Server-2 (VM)	8	64 GB	500 GB
11	Sftp-Server-3	8	64 GB	1 TB
12	Test-DB-Server	4	256 GB	6 TB
13	Test-App-Server	12	128 GB	1 TB
14	Git-Server (VM)	8	64 GB	300 GB
15	Publishing-Server (VM)	8	64 GB	300 GB
16	DR-DB (at SDC)	8	512 GB	6TB
17	SAN details—HP 3 PAR			Approx. 50 TB
18	Existing OS Software Licenses – MS Windows Server 2019 Standard, Oracle Linux 7.X			

Serial No.	Name	No. of License (For database)
1	Oracle Active Data Guard - Processor Perpetual	24
2	Oracle Diagnostics Pack - Processor Perpetual	24
3	Oracle Tuning Pack - Processor Perpetual	24

4	Oracle Database Enterprise Edition - Processor Perpetual	24
5	Oracle Database Enterprise Edition - Named User Plus Perpetual	25
6	Oracle Real Application Clusters - Processor Perpetual	12

Network-Components

Serial No	Name	Specification
1	NGFW Firewall	Fortigate-NGFW-2601F (In HA)
2	Sandbox	Forti sandbox 1000F (In HA)
3	Log Analyzer	Forti analyser 300G
4	Leased Line	512 Mbps between FDC and SDC, ITDA (Tata and BSNL) (In HA)

Note- Generally the system(www.ifms.uk.gov.in) is at its peak during 25th to 5th of every month with 250 transactions per second (TPS). The concurrent sessions on database during peak hours are generally between 900 to1000 sessions. Simultaneously around 7 Lakhs users can access the Software during peak time.

Network load- 21,166,820 average session per day.

7. Conditions under which this EoI is issued

1. This EoI is not an offer and is issued with no commitment. DTPE reserves the right to withdraw the EoI and change or vary any part thereof at any stage. DTPE also reserves the right to disqualify any bidder, should it be so necessary at any stage.
2. DTPE reserves the right to withdraw this EoI if DTPE determines that such action is in the best interest of the Government of Uttarakhand.
3. The bidder must meet the eligibility criteria to qualify for the next stage.
4. Short-listed bidders would be issued formal tender enquiry/Request for Proposal inviting their technical and commercial bids at a later date.
5. No oral conversations or agreements with any official, agent, or employee of DTPE shall affect or modify any terms of this EoI and any alleged oral agreement or arrangement made by a bidder with any department, agency, official or employee of DTPE shall be superseded by the definitive agreement that results from this EoI process. Oral communications by DTPE to bidders shall not be considered binding on DTPE, nor shall any written materials provided by any person other than DTPE.
6. Neither the bidder nor any of the bidder's representatives shall have any claims whatsoever against DTPE or any of their respective officials, agents, or employees arising out of, or relating to this EoI or these procedures (other than those arising under a definitive service agreement with the bidder in accordance with the terms thereof).
7. Applicants who are found to canvass, influence or attempt to influence in any manner the qualification or selection process, including without limitation, by offering bribes or other illegal gratification, shall be disqualified from the process at any stage.
8. The bidders are required to submit the EoI in specified format furnishing all the required

information and supporting documents.

9. Each applicant shall submit only one EoI proposal.

8. Acknowledgement of understanding of terms

By submitting a proposal, each bidder shall be deemed to acknowledge that it has carefully read all sections of this EoI, including all forms, schedules and annexure hereto, and has fully informed itself as to all existing conditions and limitations.

9. Evaluation of EOI

The bidders' EoI Proposal will be evaluated as per the eligibility criteria specified in the EoI document. The Bidders are required to submit all required documentation in support of the eligibility criteria specified (e.g. detailed project citations and completion certificates, client contact information for verification, profiles of project resources and all others) as required for evaluation. Successful bidders at EoI stage will be intimated for participation in the next stage of the bidding process.

10. Language of the proposal

The proposal and all correspondence and documents shall be written in English.

11. Solution for cloud environment

As per the format given in the Annexure I, the bidder has to provide a detailed solution plan for hosting IFMS software in the MeitY empaneled Cloud environment. The solution plan should include information on the hardware (vCPU, RAM, and storage) that will be used, the bring-your-own-license (BYOL) strategy that will be employed, and the database leveraging technologies that will be utilized. The proposed solution should also elaborate the migration plan, roll back plan, fall-back plan, disaster recovery (DR) and business continuity plan etc. These plans should provide a clear overview of the steps that will be taken to ensure successful deployment and operation of the IFMS software in the MeitY cloud environment, as well as measures to mitigate potential risks or issues.

12. Exit Management / Transition Out Requirements

In addition to the solution plan, the bidder shall also provide an exit management plan as part of the proposed solution, in accordance with Meity Cloud Guidelines. The exit plan should outline the process and steps for transitioning out of the Meity Cloud environment and the associated costs. Additionally, the bidder should also indicate whether there are any additional costs associated with the Exit/Transition out process and provide a detailed explanation of these costs.

13. Pre-Bid Queries:

DTPE will entertain the pre-bid queries from the prospective bidder through https://uktenders.gov.in/ in the format attached at annexure V table 9 .The bidder may submit the

queries through email at treas-ua@nic.in before the last date of submission of queries in the format given at annexure V Table 9.The bidder may also contact at Finance Data Center,23 Laxmi Road, Dalanwala, Dehradun Uttarakhand 248001,and Phone:0135–2226852, 2226857, 2226826. No query will be entertained after the last date of submission of queries.

.

14. Right to terminate the EOI Process

DTPE makes no commitments, explicit or implicit, that this process will result in a business transaction with anyone. Further, this EOI does not constitute an offer by DTPE. The bidder's participation in this process may result in DTPE selecting the bidder to engage in further discussions and negotiations (financial or otherwise) towards execution of a contract. The commencement of such negotiations does not, however, signify a commitment by DTPE to execute a contract or to continue negotiations.

15. Rights to the Content of the Proposal

For all the bids received before the last date and time of bid submission, the proposals and accompanying documentation of the proposal will become the property of DTPE and will not be returned after opening of the EoI proposals. DTPE 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. DTPE 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.

16. Modification and Withdrawal of Proposals

No proposal may be withdrawn in the interval between the deadline for submission of proposals andtheexpirationofthevalidityperiodspecifiedbythebidderontheproposalform.

17. Non-Conforming Proposals

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

- If it does not comply with the requirements of this EOI.
- If it fails to comply with the requirements, and acknowledgment of receipt of amendments, are common causes for holding proposals non-conforming
- If a proposal appears to be "canned" presentations of promotional materials that do not follow the format requested in this EOI or do not appear to address the requirements of the proposed solution, and any such bidders may also be disqualified.

18. Disqualification

The proposal is liable to be disqualified in the following cases or in case bidder fails to meet the bidding requirements as indicated in this EOI:

❖ Proposal not submitted in accordance with the procedure and formats prescribed in this document or treated as non-conforming proposal.

❖ During validity of the proposal, or its extended period, if any, the bidder increases its

quoted prices.

- ❖ The bidder qualifies the proposal with its own conditions.
- ❖ Proposal is received in incomplete form.
- ❖ Proposal is received after due date and time at the designated venue.
- ❖ Proposal is not accompanied by all the requisite documents.
- ❖ If bidder provides quotation only for a part of the project.
- ❖ Information submitted for Eligibility and/or in Technical Proposal is found to be misrepresented, incorrect or false, accidentally, unwittingly or otherwise, at any time during the processing of the contract (no matter at what stage) or during the tenure of the contract including the extension period if any.
- ❖ Bidder tries to influence the proposal evaluation process by unlawful/ corrupt/ fraudulent means at any point of time during the bid process.
- ❖ In case any one bidder submits multiple proposals or if common interests are found in two or more bidders, the bidders are likely to be disqualified, unless additional proposals/ bidders are withdrawn upon notice immediately.

19. Right to Accept Any Proposal and To Reject Any or All Proposal (s)

DTPE reserves the right to accept or reject any proposal, and to annul the procurement process and reject all proposals at any time prior to award of Work Order, 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 DTPE action.

Notification of Award-Prior to the expiration of the validity period of this EOI, DTPE will notify the successful bidder in writing or by fax or by email, that its proposal has been accepted. In case the EOI process has not been completed within the stipulated period, DTPE, may like to request the bidders to extend the validity period of the bid.

20. Fraud and Corrupt Practices

DTPE requires that Bidders participating under this EOI Document must observe the highest standards of ethics during the procurement process. In pursuance of this policy, DTPE:

Defines, for the purposes of this provision, the terms set forth as follows:

- "Corrupt practice" means the offering, giving, receiving or soliciting of anything of value to influence the action of DTPE or any personnel of Bidders participating in this EOI.
- "Fraudulent practice" means erroneous presentation of facts, in order to influence a procurement process or the execution of a contract, to DTPE, and includes collusive practice among Respondents (prior to or after Proposal submission) designed to establish Proposal prices at artificially high or non-competitive levels and to deprive DTPE of the benefits of free and open competition;
- ” Coercive practices” means harming or threatening to harm, directly or indirectly, persons or their property to influence their participation in the EOI and/or execution of the contract.
- Will reject a proposal for award, if it determines that the Bidder recommended for award, has been determined by DTPE to have been engaged incorrupt, fraudulent or coercive practices.
- Will declare a firm or any of its partner organizations ineligible, either indefinitely or for a

stated period of time, for participating in future EOIs and/or awarding the contract, if it at any time determines that the firm has engaged in corrupt or fraudulent practice in competing for the EOI.

21. Term and Conditions mentioned in this EOI

In case of any conflict between any condition/part as mentioned in this EOI with that as mentioned in https://uktenders.gov.in/ for MeitY empaneled Cloud Service Provider then the conditions mentioned in this EOI will supersede.

Note: Bidders should note that the requirements given in this Expression of Interest are indicative only and DTPE will seek inputs from the short-listed bidders in further refining the requirements and all aspects of services before finalizing the Request for Proposal.

Annexure I – Format for submission of solution proposed by the bidder

Existing setup at FDC	Proposed Solution	Risk associated	Mitigation plan for all the associated risks
As per existing setup given in table-3			

Note: Bidder should note that:

The solution proposed should include information on the hardware (vCPU, RAM, and storage) that will be used, the bring-your-own-license (BYOL) strategy that will be employed, and the database leveraging technologies, storage methodologies (block, object, file, archival) that will be utilized. The proposed solution should also elaborate the migration plan, roll back plan, fall-back plan, disaster recovery (DR) and business continuity plan etc. These plans should provide a clear overview of the steps that will be taken to ensure successful deployment and operation of the IFMS software in the MeitY cloud environment, as well as measures to mitigate potential risks or issues.

Annexure II–Certificate/Undertaking from Bidder

<Bidder Company Letter head>

LETTER FOR SUBMISSION OF PROPOSAL

[Letterhead paper of the Applicant including full postal address, and telephone, facsimile and e-mail address]

Date: _____

To,
The Director
Directorate of Treasuries, Pension and Entitlement, Uttarakhand
23, Laxmi Road, Dalanwala,
Dehradun-248001

Sir,
Having examined the details given in EOI document for the above assignment, I hereby submit the relevant information for considering my proposal for engagement of my services as Vendor. I am / we are submitting proposal as a [Company registered under Indian Companies Act 1956/2013]

a) I / We hereby certify that all the statements made and information supplied in the enclosed all Annexure and accompanying statements are true and correct.
b) I / We have furnished all information and details necessary for submission of proposal and have no further pertinent information to supply.
c) I / We also authorize Director DTPE, Dehradun or their authorized representatives to approach individuals, employers and firms to verify our competence and general reputation.
d) I / We shall be liable to the Govt. of Uttarakhand for all my obligations and liabilities as per terms outlined in the EOI Documents.

Certificate from

*Signature of the Applicant/
Authorized representative

Enclosures
Seal of applicant
Date of submission

*Should be signed by lead bidder only.

Annexure III-Proforma for not being blacklisted

<Bidder Company Letterhead>

<Place>

<Date>

To,
The Director
Directorate of Treasuries, Pension and Entitlement, Uttarakhand
23, Laxmi Road, Dalanwala,
Dehradun-248001

Dear Sir,

We confirm that our company is not blacklisted in any manner whatsoever by any State Government, Central Government or any other Public Sector Undertaking or a Corporation or any other autonomous organization of Central or State Government as on bid submission date. It is hereby confirmed that I/we are entitled to act on behalf of our company/corporation/firm/organization and empowered to sign this document as well as such other documents, which may be required in this connection.

<Signature of authorized signatory>

<Name and Title of the Authorized

Signatory>On behalf of

<Bidder–Name of the Company/Agency>

<Address>

<Seal/Stamp of Bidder>

Annexure IV-Proforma for Submitting project Details

1. The bidder must submit the documents regarding projects as per the table below (To be submitted along with technical proposal)

Table 7

S. No	Name of Project	Name of the client	Scope	Start date	End Date	Page Number.	Citations

2. All the documents should be properly indexed as per the table:

Table 8

S. No	Name of Document	Description	Page Number.

Annexure V–Format for Submitting Pre-bid Queries

Table 9

S. No	Name of Document (EOI Document/ Corrigendum Number)	Topic	Page Number	Point number	Existing Clause

AnnexureVI-Eligibility Criteria Compliance Sheet

S. No.	Requirements	Evidence to be submitted~	Attached Documents (Yes/No)	Page No.
1.	Bidder must be a Legal Entity i.e. 1. A company incorporated under the Indian Companies Act,2013 or any other previous company law as per section2(20) of the Indian	Certified by Authorized Signatory: 1.Copy of Certificate of Incorporation/ Registration Copy of Registration		

	CompaniesAct2013 on or before 01-04-2017 Registered with the Income Tax (PAN) and GST (GSTN) Authorities in India with active status	Certificates with the GST & IT (PAN)Authorities		
2.	The cloud services offered by the Bidder should provide Meity empaneled Cloud Service Provider(CSP).	Valid certificate from Meity.		
3.	In case the bidder is MSP then bidder should provide undertaking from CSP regarding authorization for providing cloud services.	Undertaking from CSP. MAF of CSP and Security Services.		
4.	The Bidder should have average annual turnover of at least INR10 Crore from Cloud (CSP) and Data Centre Infrastructure services (i.e. FY2019-20, FY20-21 and FY2021-22)	CA Certified copy should be provided mentioning business from the Cloud service and Data Centre Infrastructure services.		
5.	The bidder should have positive Net worth in last 3 financial years (i.e.FY2019-20,FY20-21andFY2021-22)	Chartered Accountant certificate for Net-worth of the company. Copy of the audited profit and loss account of the company showing turnover of the company for last three years.		
6.	The Bidder should not have been blacklisted or conflict of activities by any State Government, Central Government or any other Public Sector undertaking or a corporation or any other Autonomous Organization of Central or State Government for breach of Contractual Conditions as on bid submission date.	Self-declaration from Bidder		
7.	The bidder should provide the following Cloud Security Certificates of proposed cloud service ❖ ISO27017/27018 ❖ ISO27701 ❖ ISO22301 ❖ Tier-3certification	Submit valid Copy of the Certificates at the time of bid submission.		
8.	The bidder should provide the cloud service having accreditation relevant to security, availability, confidentiality, processing, integrity and privacy trust services principles SOC1,	Third Party Audited/Applicable reports to be submitted		

	SOC2/SOC3, PCIDSS			
9.	The Bidder should have annual turnover of INR 50 Cr. For last 3 financial years (i.e. FY2019-20, FY20-21and FY 2021-22)	CA Certificate and certified copy of turnover to be submitted		
10.	The bidder must have on its roll at least 5 technically Cloud Certified professionals and prior experience in providing the Cloud/ Data Centre Infrastructure services as on 31-03- 22	a) Certificate from bidders HR Department for number of Technically qualified professionals employed by the company. b) Details of the employees to be deployed along with certified copies of Cloud certifications done.		
11.	Bidder/CSP should have Completed at least one project of cloud services/Data Center Infrastructure Services with similar nature involving hosting of financial application and database in cloud environment to any Government Organization /PSU with project cost worth more than 3.5 crore.	Copy of work order Copy of Commissioning certificate/Completion certificate		

Infrastructure as a Service (IaaS)– Compute – Virtual Machine			
S.No	**Requirements**	**Attached Documents (Yes/No)**	**Page No.**
1	CSP shall support industry Oracle Linux and windows OS.		
2	The CSP should ensure that underlying processors should not have been discontinued by the processor OEM at time of bidding and they are the latest generation of Processors.		
3	Auto scaling (Up & Down) of compute based on metrics (CPU, Memory and Storage) & time/schedule based to align with business demand like month end peak, quarterly & annual peaks.		
4.	Database required is Oracle Enterprise Edition with RAC to support Active-Active deployment to achieve high availability at database layer. It should be supported by OEM of database . It should support BYOL method.		

5.	Cloud should have capability of Automatic and manual back-ups to support point in time recovery.		
6.	Cloud should support full encryption of entire database, backups and all network connections. In addition, should provide Database auditing in terms of Login failures, Modifications to user accounts or database structures.		
7.	Data Centre and Disaster Site (DR) shall be in India but in different seismic zone at least 500 km apart from each other.		
8.	CSP should support copying snapshots of any size between different regions for disaster recovery purposes		
9.	Cloud should provide built-In Machine Learning Library like Clustering, Classification, Regression, Feature Extraction, Text Mining Support, Statistical Functions etc.		

Annexure VII- Declaration to Adherence to the Terms and Conditions outlined in the Expression of Interest Document

To,
The Director
Directorate of Treasuries, Pension and Entitlement, Uttarakhand
23, Laxmi Road, Dalanwala,
Dehradun-248001

Subject: Request for Expression of Interest (EOI) for procuring cloud services for Finance Data Center, Uttarakhand for a period of five (03) years.

Sir,

I have carefully gone through the Terms and Conditions outlined in the EOI document, regarding procuring cloud services for Finance Data Center. I declare that all the provisions of this Document are acceptable to my Company. I further certify that I am an authorized signatory of my company and am, therefore, competent to make this declaration.

Yours truly

Name: _____

Designation: _____

Company: _____

Address: _____

AnnexureVIII– Undertaking from Cloud Service Provider (CSP/MSP)

(Incase the bidder is different from the Cloud Service Provider)

(CSP/MSP letterhead) [Date]

To,
The Director
Directorate of Treasuries, Pension and Entitlement, Uttarakhand
23, Laxmi Road, Dalanwala,
Dehradun-248001

Sub: Authorization to the <Service Provider> for Providing Services based on our Cloud Services

Sir / Madam,

This is to certify that I/We am/are the Cloud Service Provider and all of our offered Cloud Service Offerings for the proposed deployment models (listed below) are provisionally empaneled with MeitY.
I/We confirm that <name of SP> ("SP") have due authorization from us to provide the cloud-based services listed below, to DTPE, as per EOI document relating to
<<Title of the EOI>>

Sr. No.	Service Offering	Deployment Model	Remarks
1.			
2.			
3.			

Yours faithfully, Authorized Signatory Designation
CSP/MSP's company name

********** END OF DOCUMENT**********