Request for Proposal (RFP)

Engagement of Cloud Service Provider [CSP] for Subhadra Application, Govt. of Odisha

RFP No. OCAC-SEGP-INFRA-0027-2024-24074

OCAC Building, Plot No.-N-1/7-D, Acharya Vihar Square,
RRL Post Office, Bhubaneswar-751013 (INDIA)
Phone: 0674-2567064/2567280, FAX: 91-0674-2567842

DISCLAIMER

The information contained in this limited RFP document or subsequently provided to Bidder(s), whether verbally or in documentary or any other form by Odisha Computer Application Centre (OCAC) or any of their employees is provided to Bidder(s) on the terms and conditions set out in this RFP Document and such other terms and conditions subject to which such information is provided.

This RFP is not an agreement and is neither an offer nor invitation by OCAC to the Bidders or any other person. The purpose of this RFP is to provide interested parties with information that may be useful to them in making their technical and financial offers pursuant to this RFP (the "Bid"). This RFP includes statements, which reflect various assumptions and assessments arrived at by the bidder in relation to the Project. Such assumptions, assessments and statements do not purport to contain all the information that each Bidder may require. The assumptions, assessments, statements and information contained in this RFP, may not be complete, accurate, adequate or correct. Each Bidder should, therefore, conduct its own investigations, studies and analysis and should check the accuracy, adequacy, correctness, reliability and completeness of the assumptions, assessments, statements and information contained in this RFP and obtain independent advice from appropriate sources.

Information provided in this RFP to the Bidder(s) is on a wide range of matters, some of which depends upon interpretation of law. The information given is not an exhaustive account of statutory requirements and should not be regarded as a complete or authoritative statement of law accepts no responsibility for the accuracy or otherwise for any interpretation or opinion on law expressed herein.

OCAC, makes no representation or warranty and shall have no liability to any person, including any Bidder under any law, statute, rules or regulations or tort, principles of restitution or unjust enrichment or otherwise for any loss, damages, cost or expense which may arise from or be incurred or suffered on account of anything contained in this RFP or otherwise, including the accuracy, adequacy, correctness, completeness or reliability of the RFP and any assessment, assumption, statement or information contained therein or deemed to form part of this RFP or arising in any way in this Bid Stage. OCAC also accepts no liability of any nature whether resulting from negligence or otherwise howsoever caused arising from reliance of any Bidder upon the statements contained in this RFP.

OCAC may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information, assessment or assumptions contained in this RFP. The issue of this RFP does not imply that is bound to select a Bidder or to appoint the Preferred Bidder, as the case may be, for the Project and reserves the right to reject all or any of the Bidders or Bids without assigning any reason whatsoever.

OCAC reserves all the rights to cancel, terminate, change or modify this selection process and/or requirements of bidding stated in the RFP, at any time without assigning any reason or providing any notice and without accepting any liability for the same.

Table of Contents

1. Introduction

OCAC invites proposals from competitive managed service providers (MSP)/ cloud service providers (CSP) for engagement to provide cloud services e.g. SaaS, PaaS, IaaS, DevOps, and DRaaS etc. to Government of Odisha.

This request for proposal document has been prepared solely for the purpose of enabling OCAC with other state government departments/ agencies to engage Cloud Service Provider for managing, support and hosting of various department /Agency/ PSU's application/ portals/ analytics services and associated application software. The RFP document is not a recommendation, offer or invitation to enter into a contract, agreement or any other arrangement, in respect of the services.

This tender document is available at www.ocac.in/ www.odisha.gov.in / www.enivida.odisha.gov.in.

Joint Venture or consortium is not allowed for the scope of work mentioned in this RFP. The response to RFP must be received not later than time, date and venue mentioned on the cover page. Bids that are received after the deadline will not be considered in this procurement process.

2. Critical Information

Bidders are advised to study the RFP document carefully before submitting their techno-commercial proposals in response to the RFP Notice.

Submission of a proposal in response to this notice shall be deemed to have been done after careful study and examination of this document with full understanding of its terms, conditions and implications.

2.1. Critical Information regarding the Bidding

SL#	Information	Details
1	**RFP Number**	OCAC-SEGP-INFRA-0027-2024-24074
2	**Earnest Money Deposit (EMD)**	EMD of ₹5,00,000/- (Rupees Five Lakhs only) in the form of Demand Draft, drawn from any Scheduled Bank in India, in favour of "Odisha Computer Application Centre", payable at Bhubaneswar or in shape of Bank Guarantee valid for 6 months from the last date of submission of bid
3	**Last date for submission of Bid**	28.10.2024, 12.30 PM
4	**Opening of Technical Bid**	28.10.2024, 12:40 PM
5	**Opening of Price Bid**	Will be intimated later

3. About Odisha Computer Application Centre (OCAC)

Odisha Computer Application Centre (OCAC), the designated Technical Directorate of Electronics & Information Technology Department, Government of Odisha, has evolved through years as a centre of excellence in ICT solutions and e-Governance. It has contributed significantly to the steady growth of ICT in the state. It helps ICT to reach the

common citizen so as to narrow down the Digital divide and spread-out applications of ICT by establishing a system where the citizens are receiving transparent governance.
Bidders may view and study this tender document containing the detailed terms & conditions from the website www.odisha.gov.in, www.ocac.in, www.enivida.odisha.gov.in and www.odisha.gov.in . The bids are to be submitted as per procedure given in this document.

4. Terms of Reference

4.1. Objective

OCAC intends to engage the Cloud Service Providers for managed support and hosting of Subhadra Application of W & CD Department and any other application required by OCAC time to time, if required.
The proposed cloud solution should be scalable, extensible, highly configurable, secure and very responsive and shall support integration and interfacing with software and solutions developed or used by OCAC or State Departments or its Directorates / associate institutions and / or other stakeholders.

4.2. General Requirements

1. Engaged MSP/ CSP ("the Bidders") shall host, deploy and operationalize the IT System Solutions as decided by the OCAC in close coordination / collaboration with OCAC.
2. The CSP must be empanelled by MeitY as Cloud Service Provider.
3. Resolve all technical issues/ queries faced by portal/ web application users.
4. Send Daily status reports and Ad hoc reports as required by the Purchaser.
5. Provide web portal/ application maintenance support 24X7X365 days.
6. Ensure that the portal/ application operations are secure and free from cyber-attacks, 24X7 proactive monitoring, protection against hacking and cyber-crimes. Thus, to provide "Safe to Host" certificate initially and then at each financial year.
7. Provide highly secured, managed, Uptime / TIA 942 Tier-3 compliant Data Centre Core Infrastructure 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.).
8. 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. This specification and quantity are minimum as required for the scope of work mentioned in this RFP. However, Bidders at their interpretations can propose infrastructure over and above this minimum specification as mentioned in this RFP.
9. The DC 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. However, SMS may not be mandatory, but notifications would be required and it should not be an impediment in meeting the SLA requirements.

10. The DC shall be physically located in India. The Bidder must provide self-certification in this regard.
11. OCAC and its appointed third-party auditors may visit the Bidder DC for auditing. The Bidder shall provide assistance and furnish the relevant information requested by the auditors.
12. Content management of the website will be managed and monitored by the Bidder.
13. No freeware software to be used unless authorised by OCAC and its associated TPAs.
14. The selected bidder should provide a declaration of data and data backup being maintained must reside in India.

4.3. Documents prepared by the Bidder to be the Property of the "OCAC"

All plans, specifications, designs, reports, and other documents prepared by the bidder for the "the Purchaser" under this Contract shall become and remain the property of the "the Purchaser", and the Bidder shall, not later than upon termination or expiration of this Contract, deliver all such documents to the "the Purchaser", together with a detailed inventory thereof. The Bidder may retain a copy of such documents, but shall not use anywhere, without taking permission, in writing, from the Purchaser and the Purchaser reserves right to grant or deny any such request. If license agreements are necessary or appropriate between the Bidder and third parties for purposes of development of any such computer programs, the Bidder shall obtain the Purchaser prior written approval to such agreements, and the "the Purchaser" shall be entitled at its. Discretion to require recovering the expenses related to the development of the program.

4.4. IT Assets and Intellectual Properties (IP) Ownership

Following table describes the ownership of various Assets and IPR Ownership. The Bidder shall submit the working code for the Software Solutions which shall be the OCAC IPR.

Table-Assets and IPR Ownership

Sl#	Application Infrastructure	HW	OS	DB	SW*	Data	Custom Solutions
1.	Storage	CSP	CSP	NA	CSP	OCAC	NA
2.	Software Update Service	CSP	CSP	CSP	CSP	OCAC	NA
3.	Portal software	CSP	CSP	CSP	OCAC	OCAC	OCAC
4.	Analytics	CSP	CSP	CSP	CSP	OCAC	CSP
5.	Incident & Change Management	CSP	CSP	NA	CSP	OCAC	CSP
Dashboards & Analytics – if these are Commercially available packaged software, then only the customized source code or module shall be treated as OCAC IP and working code shall be submitted. Bidder - Bidder provided (Managed Data Center, IaaS, PaaS or SaaS) OCAC - OCAC owns this as asset. * indicates System software, database software, commercially available tools and software							

4.5. Responsibility Matrix

The Responsibility Matrix showing the responsibility of Bidder, Application vendor (if existing) and OCAC is placed below:-

Table- Responsibility Matrix

Sl#	Activity	CSP/MSP	Application vendor (if any)	OCAC
1.	Understanding Application Architecture (Existing /New)	**Y**	**Y**	
2.	Design of Cloud Solution according to application	**Y**		
3.	Procurement of additional user Software licenses and installation according to application	**Y**		
4.	Installation of Application Software /Web portal/ Web Application	**Y**		
5.	Installation and updating the Operating Systems	**Y**		
6.	Installation and updating the Databases	**Y**		
7.	Installation and updating the middleware (if any)	**Y**		
8.	Configuration of Cloud Solution	**Y**		
9.	Provisioning of the required hardware for IaaS Cloud	**Y**		
10.	Network Connectivity to IaaS Cloud	**Y**		
11.	Internet Connectivity provisioning IaaS Cloud	**Y**		
12.	Migration of application from existing cloud setup to new cloud	**Y**	**Y**	
13.	Infrastructure Testing	**Y**		
14.	Data Integrity Testing	**Y**		
15.	Cloud Solution Functional Testing	**Y**	**Y**	**Y**
16.	Switch Over Testing	**Y**		
17.	Switch Over Testing	**Y**		
18.	Cloud Solution Maintenance	**Y**		
19.	Cloud Service Provisioning through Self Service Portal /API	**Y**		
20.	24x7x365 Support, Cloud service Provisioning, de-provisioning, up-dation, auto-scaling etc.	**Y**		
21.	Maintenance & Management of Cloud Solution & infrastructure post implementation	**Y**		

5. Cloud Service Provisioning Requirements

5.1. Virtual Machines and Compute:

5.1.1. Virtual Machines

Virtual Machines	
Requirement	**Description**
Compute instances – • General Purpose • Memory optimized • Compute optimized • Storage optimized • GPU instances	Cloud provider should offer the following instance types – • General Purpose – optimized for generic applications and provides a balance of compute, memory, and network resources • Memory optimized – optimized for memory applications • Compute optimized – optimized for compute applications

	• Storage optimized – include very fast/large amount of local storage for NoSQL databases and Hadoop • GPU – intended for graphics and general-purpose GPU compute applications
Compute instances –Burstable performance	Cloud provider should offer instances that provide a baseline level of CPU performance with the ability to burst above the baseline.
Compute instances – Nested Virtualization	Cloud provider should offer instances that can run nested virtual machines, that is virtual machine inside a virtual machine.
Instance affinity – logical grouping of instances within a single data centre	Customer should be able to logically group instances together for applications that require low network latency and/or high network throughput.
Instance anti-affinity -two or more instances hosted in different data centres	Customer should be able to split and host instances across different physical data centres to ensure that a single physical failure event does not take all instances offline.
RAM size support in VMs	Cloud provider should offer VMs with up to 12 TB size.
VM Generation Support	Cloud provider should be able to support running Generation 1 & 2 virtual machines natively

5.1.2. Confidential Virtual Machines

Confidential Virtual Machines	
Requirement	**Description**
Compute instances – • General Purpose • Memory optimized • Compute optimized • Storage optimized • GPU instances	Cloud provider should offer the following instance types – • General Purpose – optimized for generic applications and provides a balance of compute, memory, and network resources • Memory optimized – optimized for memory applications • Compute optimized – optimized for compute applications • Storage optimized – optimised for storing of filesystems • GPU – intended for graphics and general-purpose GPU compute applications
Compute instances –Burstable performance	Cloud provider should offer instances that provide a baseline level of CPU performance with the ability to burst above the baseline.
Compute instances – Nested Virtualization	Cloud provider should offer instances that can run nested virtual machines, that is virtual machine inside a virtual machine.
Instance affinity – logical grouping of instances within a single data centre	Customer should be able to logically group instances together for applications that require low network latency and/or high network throughput.
Instance anti-affinity -two or more instances hosted in different data centres	Customer should be able to split and host instances across different physical data centres to ensure that a single physical failure event does not take all instances offline.
RAM size support in VMs	Cloud provider should offer VMs with up to 12 TB size.
VM Generation Support	Cloud provider should be able to support running Generation 1 & 2 virtual machines natively

5.2. Storage Services

5.2.1. Block Storage

Block Storage	
Requirement	**Description**

Support for storage allocated as local disk to a single VM	Cloud provider should offer persistent block level storage volumes for use with compute instances.
Storage volumes > 1 TB	Cloud provider should offer block storage volumes greater than 1 TB in size.
Encryption using provider managed keys	Cloud service should support encryption of data on volumes, disk I/O, and snapshots using industry standard AES-256 cryptographic algorithm.
Encryption using customer managed keys	Cloud service should support encryption using customer managed keys.
Durable snapshots	Cloud service should support point-in-time snapshots. These snapshots should be incremental in nature.
Ability to easily share snapshots globally	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.
Attach more than one compute instance to a single volume	Cloud service should support adding more than one compute instance to a single storage volume in R/W mode so that many users can access and share a common data source.
Consistent Input Output per second (IOPS)	Cloud service should support a baseline IOPS/GB and maintain it consistently at scale
Annual Failure Rates <0.01%	Cloud service should be durable and support annual failure rates of less than 0.01%, and the information must be publicly disclosed
Storage uptime	Block Storage with minimum monthly uptime of 99.99% or higher (as published in the CSP's Public Portal)

5.2.2. Object Storage

Object Storage	
Requirement	**Description**
Support for Server-side Encryption	Cloud service should support encryption for data at rest using 256-bit Advanced Encryption Standard (AES-256) encryption to encrypt your data.
Support for Server Side Encryption with Customer-Provided Keys	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.
Support for Server Side Encryption with a Key Management Service	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.
Object lifecycle management	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.
High-scale static web site hosting	Cloud service should be able to host a website that uses client-side technologies (such as HTML, CSS, and JavaScript) and does not require server-side technologies (such as PHP and ASP.NET).

Object Versioning	Cloud Service should support versioning, where multiple versions of an object can be kept in one bucket. Versioning protects against unintended overwrites and deletions.
Flexible access-control mechanisms	Cloud service should support flexible access-control policies to manage permissions for objects.
Audit logs	Cloud service should be able to provide audit logs on storage buckets including details about a single access request, such as the requester, bucket name, request time, request action, response status, and error code.
Accidental deletion prevention	CSP should offer a mechanism to avoid accidental deletion of data. In such case data when deleted should be preserved for a minimum of 2 weeks.
Strong Consistency	Cloud service should support read-after-write consistency for PUT operations for new objects.
Storage gateway appliance for automated enterprise backups	Cloud provider should offer a storage gateway appliance for seamlessly storing on-premises data to the cloud.
Durability	Object storage should be replicated across multiple DC's for better resiliency and should be designed for 99.99% availability and 99.99999999999999% (16 9's) durability.

5.3. Managed Database as a Service

5.3.1. Managed Database Service

Managed Database Service – PostgreSQL	
Requirement	**Description**
Support for PostgreSQL	Cloud service should support the last two major releases of PostgreSQL
Read Replica support	Cloud service should support up to 5 read replicas that make it easy to elastically scale out beyond the capacity constraints of a single DB Instance for read-heavy database workloads.
Read Replica support	Cloud service should support having read replicas in different region in India, that should be more than 100 Km from DC.
Manual Failover	Cloud service should support a manual failover of the DB instance from primary to a standby replica.
Cross region Snapshots	Cloud service should support copying snapshots of any size between different cloud provider regions for disaster recovery purposes.
Cross region Read Replica	Cloud service should support creating multiple in-region and cross-region replicas per database instance for scalability or disaster recovery purposes.
High Availability	Cloud Service should support enhanced availability and durability for database instances for production workloads.
Point in time restore	Cloud service should support restoring a DB instance to a specific date and time.
User snapshots and restore	Cloud service should support creating a DB snapshot and restoring a DB instance from a snapshot.
Modifiable DB parameters	Cloud service should allow the DB parameter to be modified.
Monitoring	Cloud service should allow monitoring of performance and health of a database or a DB instance.

Encryption at rest	Cloud service should support encryption using the industry standard AES-256 encryption algorithm to encrypt data.

5.4. Data Transformation and processing

1. Capability to operate on latest versions of Apache Spark and seamlessly integrate with open-source libraries
2. Capability of version control of notebooks with GitHub
3. Capability for One-click access to preconfigured machine learning environments for augmented machine learning with state-of-the-art and popular frameworks such as PyTorch, TensorFlow, and scikit-learn.
4. Capability to support for Python, Scala, R, and SQL, as well as deep learning frameworks and libraries like TensorFlow, Pytorch, and Scikit-learn
5. Capability to Track and share experiments, reproduce runs, and manage models collaboratively from a central repository
6. Capability to support for Scala, Java, R, and Python alongside Spark SQL, GraphX, Streaming, and Machine Learning Library (Mllib)
7. Capability of having built-in integration to SQL DW and therfore capability to write directly to SQL DW
8. Capability to bring data reliability and scalability to the existing data lake with an open-source transactional storage layer designed for the full data lifecycle

5.5. Data Governance and Management

1. Capability to scan the data sources and capture the schema and metadata.
2. Capability to allows users to schedule data source scans on a weekly or monthly frequency.
3. Capability to classify the captured data automatically using the default rules or based on user-defined custom data classification rules.
4. Capability to allows the users to view a map of the data lifecycle e.g. for ETL system , users are able to see how the data flows from the source to the final sink.
5. Capability to provide extensive search and browsing capabilities, for better collaboration and reusability of existing data assets in the organization
6. Capability to navigate easily to view the related data assets.
7. Capability with a built-in Insights report that provides a high-level view of the data estate, such as, scan insights, classification insights, file extension insights etc

5.6. Artificial Intelligence and Machine Learning

1. Capability to use a model built from an open-source platform, such as Pytorch, TensorFlow, or scikit-learn
2. Capability to allow users to define repeatable and reusable steps for their data preparation, training, and scoring processes.
3. Capability to Create reusable software environments for training and deploying models
4. Capability to Register, package, and deploy models from anywhere.

5. Users can also track associated metadata required to use the model.
6. Capability to Capture the governance data for the end-to-end ML lifecycle.
7. Capability to Notify alerts on experiment completion, model registration, model deployment, and data drift detection
8. Capability to Compare model inputs between training and inference, explore model-specific metrics, and provide monitoring and alerts on their ML infrastructure.
9. Capability in using pipelines that allows user to frequently update models, test new models, and continuously roll out new ML models alongside their other applications and services.
10. Capability to Use automated machine learning, which accepts configuration parameters and training data
11. Capability to Create, manage, and monitor labelling projects, and automate iterative tasks with machine learning–assisted labelling.
12. Capability to Perform interactive data preparation with PySpark
13. Capability of model interpretability to understand how the model was built.
14. Capability to Maximize productivity with IntelliSense, easy compute and kernel switching, and offline notebook editing
15. Capability to Use machine learning tools like designer for data transformation, model training, and evaluation, or to easily create and publish machine learning pipelines.
16. Capability to perform Scale reinforcement learning to powerful compute clusters, support multiple-agent scenarios, and access open-source reinforcement learning algorithms, frameworks, and environments.
17. Capability to Get model transparency at training and inferencing with interpretability capabilities
18. Capability to Improve model reliability and identify and diagnose model errors with the error analysis toolkit.
19. Capability to Automatically capture lineage and governance data with audit trail
20. Capability to Use Git integration to track work and GitHub Actions support to implement ML workflows.
21. Capability to manage endpoints to operationalize model deployment and scoring, log metrics, and perform safe model rollouts.
22. Capability to manage compute to distribute training and to rapidly test, validate, and deploy models.
23. Capability to Share CPU and GPU clusters across a workspace and automatically scale to meet your machine learning needs.
24. Capability to run machine learning on existing Kubernetes clusters on premises, in multicloud environments, and at the edge with Azure Arc.
25. Capability to Build and deploy models more securely with network isolation and end-to-end private IP capabilities, role-based access control for resources and actions, custom roles, and managed identity for compute resources.

5.7. Virtual Firewall and Information Security Services

1. Capability to protect servers based on protocols and ports.
2. Capability to protect network subnets with access controls that provides an optional layer of security that provides a stateless firewall for controlling traffic in and out of a subnet
3. Capability to segregate public subnet and private subnet
4. Capability to configure route tables that define which subnets are allowed to route external traffic over backend VPN or site-site connections, Cloud Infrastructure peering connections, Internet connections, or even specific virtual machine instances.
5. Prevent packet sniffing: Virtual instances should be designed to prevent other instances running in promiscuous mode to receive or "sniff" traffic that is intended for a different virtual instance. Even if tenants configure interfaces into promiscuous mode, the hypervisor should not deliver any traffic to them that is not addressed to them.
6. Prevent IP Spoofing: the cloud service should not permit an instance to send traffic with a source IP or MAC address other than its own.

5.8. Server Security & HIPS (Host-based Intrusion Prevention System)

1. The server security solution should support stateful Inspection Firewall, Antimalware, Deep Packet Inspection with HIPS, Integrity Monitoring and Recommended scan in single agent for physical, virtual and cloud instances.
2. The server Security solution should provide automatic recommendations against existing vulnerabilities, dynamically tuning IDS/IPS sensors (Eg. Selecting rules, configuring policies, updating policies, etc.) And provide automatic recommendation of removing assigned policies if vulnerability no longer exists - For Example - If a patch is deployed unwanted signatures should be un-assigned automatically.
3. The server Solution should have an intuitive rule creation and modification interface includes the ability to include or exclude files using wildcards filenames, control over inspection of sub-directories, and other features and Solution Should have pre and post execution machine Learning and should have Ransomware Protection in behaviour Monitoring.
4. The Server Security Host based IPS should support virtual patching both known and unknown vulnerabilities until the next scheduled maintenance window.
5. Should support prevention against script-based attacks used to deliver malware such as ransomware
6. The server security solution should protect against Distributed DoS attack and Solution should have the ability to lock down a computer (prevent all communication) except with management server.
7. The Server security HIPS Solution Should not have the need to provision HIPS Rules from the Policy Server as the Rules should be automatically Provisioned and recommended according to vulnerabilities.

8. The Server Security solution should support pre-defined lists of critical system files for various operating systems and/or applications (web servers, dns, etc.) and support custom rules as well.

5.9. Security Services

1. Web Application Firewall (Layer 7):
    a. Protection from attacks by filtering traffic based on rules that you create.
    b. Filter web requests based on IP addresses, HTTP headers, HTTP body, URL, or URI strings, which allows you to block common attack patterns, such as SQL injection or cross-site scripting that could affect application availability, compromise security, or consume excessive resources.
    c. Features like protection against Web Traffic visibility, east of deployment and maintenance, integrated security.
2. DDoS Protection:
    a. Managed DDoS protection service that defends against most common, frequently occurring network and transport layer DDoS attacks that target web site or applications.
    b. When used with Content Delivery Network and global DNS service, should provide comprehensive availability protection against all known infrastructure (Layer 3, 4 and 7) attacks.
    c. Should provide always-on detection and automatic inline mitigations, minimize application downtime and latency.
3. Identity and Access Management:
    a. Service that properly separates users by their identified roles and responsibilities, thereby establishing least privilege and ensuring that users have only the permissions necessary to perform their assigned tasks. It should be accessed through Role Based Access Control.
4. Managed Threat Detection Service:
    a. Continuously monitor for malicious or unauthorized behaviour to protect accounts and workloads.
    b. It should monitor for activity such as unusual API calls or potentially unauthorized deployments that indicate a possible account compromise.
    c. The service should also detect potentially compromised instances or reconnaissance by attackers.
    d. Availability of OpenAPI based REST Services, self-service cloud portal and Command Line interface for managing cloud resources. This should be available for at least- Virtual machine, managed databases, managed NoSQL DB, Container as a service, managed queue, Storage disks, object storage, file share, network, backup, disaster recovery replication, infrastructure as code, infrastructure & security monitoring
    e. Cloud Service Providers must offer Cloud native turnkey SIEM offering to configure real-time analysis and alerting of security events. At a minimum, the

integration or service must support alerting, log retention and some form of forensic analysis that is able to search across logs and periods of time for patterns.

f. In case of requirement, the CSP/MSP should share SIEM log with OCAC.

g. CSP should provide cloud Content Delivery Network (CDN) that provides fast, reliable, and secure access between your users and your applications' static and dynamic web content across the globe. It should leverage global edge network with hundreds of global and local points of presence (PoPs) distributed around the world. Key features should include:
   - Global Delivery Scale: Use global Cloud CDN and WAN, leveraging over 100 edge locations across 100 metro cities connected to CSP's datacentres using a private enterprise-grade WAN
   - Performance: Improve latency for applications by up to 3 times using anycast network and split TCP connections
   - Security: Offer platform-level protection against network-level DDoS attacks and integrates with other cloud services such as DNS, Web Apps, and Storage for domain and origin management
   - Features: Includes SSL offload, URL redirect and rewrite, HTTP/2, IPv6 support, session affinity, simple domain onboarding with free or custom SSL certificates, caching

5. The CSP should have cloud service for securely storing and accessing secrets, such as API keys, passwords, certificates, and cryptographic keys. This helps enhance data protection and compliance by providing secure key management. The service should allow to create and import encryption keys in minutes and manage them centrally. It should use FIPS 140-2 Level 2 and Level 3 validated HSMs (Hardware Security Modules) for enhanced security
6. The CSP should have a cloud-native application protection platform (CNAPP) designed to protect cloud-based applications from various cyber threats and vulnerabilities. It should combine the capabilities of a development security operations (DevSecOps) solution that unifies security management at the code level across multicloud and multiple-pipeline environments. It also includes a cloud security posture management (CSPM) solution that surfaces actions to prevent breaches and a cloud workload protection platform (CWPP) with specific protections for servers, containers, storage, databases, and other workloads
7. The CSP should provide a fully managed, in-memory cache service provided by. It should be designed to improve the performance and scalability of applications by providing super-fast data access.

5.10. Cloud Monitoring & Management Services

1. Cloud Resource Monitoring: Capability to monitor cloud environment centrally, custom monitoring metrics, monitor and store logs, view graphs & statistics, set alarms, monitor and react to resource changes. Support monitoring of custom metrics

generated by your applications and services and any log files your applications generate. Gain system-wide visibility into resource utilization, application performance, and operational health, using these insights to react intelligently and keep applications running smoothly.

2. Audit Trail: Logs of all user activity within a CSP account including actions taken through the CSP's Management Console, CSP's SDKs, command line tools, and other CSP services. The recorded information includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the Cloud service.
3. Cloud Advisor: Analyses the Cloud environment and provides best practice recommendations (or checks) in five categories: cost optimization, security, fault tolerance, performance, and service limits.

5.11. Cloud Management Portal

The Cloud Management Portal / Self provisioning portal including but not limited to:

1. User Roles & Rights: SSCL should be able to create users based on roles & rights.
2. Monitoring Reports
3. SLA Reports
4. Backup Reports
5. VM Status report
6. Provisioning /De-provisioning of VM’s
7. Creating templates for VM’s
8. Able to make changes in configurations.

5.12. Backup Services

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

5.13. Developer Tool:

The CSP should provide a comprehensive suite of tools and services to support software development and delivery. Here are some key specifications:

1. Continuous Integration and Continuous Delivery (CI/CD): Supports any platform with unlimited free repositories and manual and exploratory testing
2. Hosted Agents: Run on general-purpose virtual machines with a 2-core CPU, 7 GB of RAM, and 14 GB of SSD disk space
3. Requirements Management: Allow capturing, analyzing, prioritizing, tracking, and collaborating on project requirements using work items
4. Security and Monitoring: Include services like firewall, DDoS protection, endpoint detection and response (EDR), vulnerability assessment and penetration testing (VAPT), and security information and event management (SIEM) with security orchestration, automation, and response (SOAR)

5.14. Support Services

1. CSP should provide direct profession support to the customer.
2. CSP support scope should include business critical dependence
3. CSP support should include billing and subscription management support
4. CSP support should include 24/7 SELF-HELP RESOURCES, INCLUDING PORTAL HOW-TO VIDEOS, DOCUMENTATION, AND COMMUNITY SUPPORT
5. CSP support should allow an infinite number of support ticket submission
6. CSP should also provide THIRD-PARTY SOFTWARE SUPPORT WITH INTEROPERABILITY AND CONFIGURATION GUIDANCE AND TROUBLESHOOTING
7. CSP should provide 24/7 ACCESS TO TECHNICAL SUPPORT BY EMAIL AND PHONE AFTER A SUPPORT REQUEST IS SUBMITTED
8. Case severity and response time should include
    - Minimal business impact (Sev C): within four business hours
    - Moderate business impact (Sev B): Within two hours
    - Critical business impact (Sev A): Within one hour

6. Cloud Infrastructure Scope of Work

6.1. Bill of Material required for Cloud hosting of Subhadra Application

SL#	Service category	Service type	Custom name	Region	Description	Qty	Unit
1.1	Compute	Virtual Machines	CI/CD VM	Central India	1 D4a v4 (4 vCPUs, 16 GB RAM), Linux; 1 managed disk – S6; Inter Region transfer type, 5 GB outbound data transfer from Central India to East Asia	1	No
1.2	Compute	Virtual Machines		Central India	D64s v4 (64 vCPUs, 256 GB RAM) x 730 Hours (Pay as you go), Linux, (Pay as you go); managed disks – E30; Inter Region transfer type, 5 GB outbound data transfer from Central India to East Asia	9	No
2.1	Storage	Storage Accounts	Document Store	Central India	Block Blob Storage, General Purpose V2, Flat Namespace, LRS Redundancy, Hot Access Tier, 100 TB Capacity, 1,000 x 10,000 Write operations, 1 x 10,000 List and Create Container Operations, 10,000 x 10,000 Read operations, 1 x 10,000 Other operations. 1,000 GB Data Retrieval, 1,000 GB Data Write, SFTP disabled	1	No
2.2	Storage	Storage Accounts	Angular - Static Web Site	Central India	Block Blob Storage, General Purpose V2, Flat Namespace, LRS Redundancy, Hot Access Tier, 100 GB Capacity - Pay as you go, 100 x 10,000 Write operations, 1 x 10,000 List and Create Container Operations, 1,000 x 10,000 Read operations, 1 x 10,000 Other operations. 1,000 GB Data Retrieval, 1,000 GB Data Write, SFTP disabled	1	No
3.1	Networking	Azure Front Door	CDN + WAF + TLS + Geo		Azure Front Door Premium - Base instance included, 1 TB Data Transfer Out to Client, 100 GB Data Transfer In to Origin, 1000 x 10,0000 Requests	1	No
3.2	Networking	Network Watcher	Network Monitoring	Central India	10 GB Network Logs Collected, 1000 Checks for Network Diagnostics, 10 Connection Metrics, 1 DNS or App Gateway Servers x 50 GB logs ingested, 1 GB logs collected for Traffic Analytics (Standard processing), 1 GB logs collected for Traffic Analytics (Accelerated processing)	1	No
3.3	Networking	Bandwidth	Egress for External API		Internet egress, 500 GB outbound data transfer from Central India routed via Microsoft Global Network	1	No
3.4	Networking	Azure Firewall		Central India	Standard tier, 1 Logical firewall units, 50 TB Data processed	1	No

3.5	Networking	VPN Gateway		Central India	VPN Gateways, Basic VPN tier, 10 S2S tunnels, 128 P2S connections, 0 GB, Inter-VNET outbound VPN gateway type	1	No
3.6	Networking	Azure DDoS Protection		Central India	Network Protection, Protection for 100 resources	1	No
3.7	Networking	Load Balancer		Central India	Standard Tier: 5 Rules, 1,000 GB Data Processed	3	No
4.1	Security	Key Vault	Encryption Key Storage	Central India	Vault: 10,000 operations	1	No
4.2	Security	Microsoft Defender for Cloud	CSPM	Central India	Microsoft Defender for Cloud Security Posture Management: 8 Billable Resources	1	No
4.3	Security	Microsoft Defender for Cloud	Anti-Malware	Central India	Microsoft Defender for Cloud Workload Protection: 9 Plan 1 servers x 730 Hours, 1 PostgreSQL Instance, 2 Storage accounts x 730 Hours with, Defender for APIs – Plan 1 with 1 estimated API monthly transactions, 1 Key Vault(s)	1	No
5.1	Databases	Azure Database for PostgreSQL	Database	Central India	Flexible Server Deployment, General Purpose Tier, 1 D16ads v5 (96 vCores) x 730 Hours (Pay as you go), Storage - Premium SSD v2, 6128 GiB Disk size, 2000 Additional IOPS, 1000 Additional throughput MBps, 3 TiB Additional Backup storage - LRS redundancy, with High Availability	1	No
5.2	Databases	Azure Database for PostgreSQL	Read	Central India	Flexible Server Deployment, General Purpose Tier, 1 D96ads v5 (96 vCores) x 730 Hours (Pay as you go), Storage - Premium SSD v2, 6128 GiB Disk size, 2000 Additional IOPS, 1000 Additional throughput MBps, LRS redundancy, without High Availability	1	No
5.3	Databases	Azure Cache for Redis		Central India	Enterprise tier: x1 scale factor (capacity 2) x 1 E5 instances x 730 Hours, Pay as you go, Software IP cost is included - Central India	1	No
6.1	Developer tools	Azure DevOps	CI CD Pipeline		1 Basic + Test Plans license users, Paid tier - 1 Microsoft Hosted Pipeline(s), 1 Self Hosted Pipeline(s), 1 GB Artifacts, 1 GitHub Advanced Security committers	1	No
6.2	DevOps	Azure Monitor	Monitoring and APM	Central India	Log analytics: Log Data Ingestion: 5 GB Daily Analytics logs ingested, 15 GB Daily Basic logs ingested, 1 months of Interactive Data Retention, 10000 Prometheus	1	No

					metrics per node, 30 seconds of Metric collection interval, 7 Dashboards, 50000 Data samples queried per dashboard, 25 promql alerting rules, 25 promql recording rules; Application Insights: 3 months Data retention, 5 Minutes Execution frequency, Executing for 1 month ; resources monitored X 1 metric time-series monitored per resource, 5 Minutes Log Signal frequency with log signals monitored and {2} time series per signal, 10 Additional events (in thousands)		
6.3	IP Addresses			Central India	Global (ARM), 5 Static IP Addresses X 730 Hours, 5 Public IP Prefixes X 730 Hours	1	No
7.1	Management and governance	Azure Backup	VM Backup	Central India	Azure VMs, Standard Backup policy, 4 Instance(s) x 1 GB, LRS Redundancy, Low Average Daily Churn, 5,387 GB Average monthly backup data in Standard Tier, 313 GB Average monthly backup data in Archive Tier	1	No
7.2	Management and governance	Azure Backup	DB Backup	Central India	Azure PostgreSQL Servers, 1 Instance(s) x 100 GB, LRS Redundancy, 1,533 GB Average monthly backup data in Standard Tier	1	No
8.1	Postgresql Reporting				Power Platform for Reporting services with Power bI Licenses	1	No
9.1	Azure Support				Professional direct Support from Azure per month	12	Man-Month
10.1	Management and monitoring				24X7 Infra Management per shift cost of 8 hrs	12	Man-Month
10.2	Management and monitoring				24X7 Information Security Management per shift cost of 8 hrs	12	Man-Month
10.3	Management and monitoring				24X7 DB/Storage Management shift cost of 8 hrs	12	Man-Month
11.1	Manpower				Azure certified Manpower	12	Man-Month
12.1	Implementation				One time implementation cost for Infra & Security Setup	1	Lumpsum
13.1	Other Services				Other Services	1	Lumpsum

Note:

- **The authority reserves the right to terminate any/all of the services with prior notice to the bidder. However, the price will remain valid for 1 year and 3 months from the date of the opening of commercial bid.**
- **The authority reserves the right to negotiate the rate against any of the items.**

6.2. Cloud Infrastructure Services

Sl#	Service type	Duration
1	Cloud Infrastructure Provisioning and Configuration Service	1 time
2	Security Setup	1 time
3	Infra Monitoring	12 Months
4	Info-Sec Monitoring	12 Months
5	Database Monitoring	12 Months
6	Cloud Infrastructure Operation & Management	12 Months

Note:

- **The authority reserves the right to terminate any/all of the services with prior notice to the bidder. However, the price will remain valid for 1 year and 3 months from the date of the opening of commercial bid.**
- **The authority reserves the right to negotiate the rate against any of the items.**

6.3. Bill of Material required for Cloud hosting of Application of A & FE Department (for Cost Discovery purpose)

Sl#	Service#	Description	Qty	Unit
1.1	**Compute Services**	Virtual Machines-DB Prod-(8 vCPUs, 16 GB RAM), Linux	1	No
1.2		Virtual Machines-Machine Learning Prod (Tesla T4 GPU enabled (8 vCPUs, 56 GB RAM) , Linux	2	No
1.3		Virtual Machines-Microservices Prod-(8 vCPUs, 16 GB RAM) , Linux	2	No
1.4		Virtual Machines-Machine Learning Staging-(Tesla T4 GPU enabled (4 vCPUs, 28 GB RAM), Linux	1	No
1.5		Virtual Machines-Db+Microservices Staging-(8 vCPUs, 16 GB RAM,Linux)	1	No
2.1	**Managed Disks Services**	Managed Disks -OS Disks-128 GB SSD	10	No
2.2		Managed Disks -DB Disks-500 GB SSD with 3000 IOPS per disk	10	No
3.1	**Azure Services**	Azure OpenAI Service-Language Models, GPT-4-Turbo-128K, 25,000 x 1,000 input tokens, 15,000 x 1,000 output tokens	1	No
3.2		Azure Firewall-Network Firewall NGFW	1	No

3.3		Azure Front Door-Web Application Firewall	1	No
3.4		Azure NAT Gateway-NAT Gateway 1 TB	1	No
3.5		Azure Backup-Backup for VM	5	No
3.6		Azure DNS-DNS Service	1	No
3.7		Azure AI Translator, S1: Standard Translation with 1,000,000 translated characters	1	No
3.8		Azure DDoS Protection-Static IP Address	1	No
4.1	**Additional services**	Bandwidth-500 GB Internet eGRess	1	No
4.2		Bandwidth-Virtual Network 1 TB	1	No
4.3		Load Balancer	1	No
4.4		Load Balancer	1	No
4.5		Microsoft Defender for Cloud-EDR/AV for servers	5	No

Note:

- **The authority reserves the right to terminate any/all of the services with prior notice to the bidder. However, the price will remain valid for 1 year and 3 months from the date of the opening of commercial bid.**
- **The authority reserves the right to negotiate the rate against any of the items.**

6.4. Scope of work for Cloud Infrastructure Provisioning and Configuration Service:

6.4.1. Landing zone

1. Create an RG and vNet to deploy the cloud services.
2. Create subnets as per the architecture diagram

6.4.2. Networking Services

1. Deploy and configure Azure Application Gateway for load balancing.
2. Enable Web Application Firewall (WAF) to protect against common vulnerabilities (SQL injection, XSS).
3. Configure load balancing rules and SSL termination for secure communication

6.4.3. App Service

1. Provision an App Service as per the BOM details.
2. Set it up with 8 instances of P3V2, each with 4 cores, 14 GB RAM, and 250 GB storage. However, in case of additional requirements CSP/MSP should be able to setup the same.

6.4.4. Storage Services

1. Create and configure Storage Accounts to store unstructured data in Blob Storage.

6.4.5. Database Services

1. Provision Azure Database for PostgreSQL as per BOM

6.4.6. Azure Firewall

1. Deploy Azure Firewall to control inbound/outbound traffic.
2. Define network security groups (NSG) and firewall policies.

6.4.7. Azure Monitor

1. Implement monitoring for virtual machines and workloads using Azure Monitor

6.4.8. Azure DevOps

1. Enable Azure DevOps Organization and integrate with the subscription using a Service connection.
2. Configure 2 CI CD pipelines to deploy the services in Production App services.

6.4.9. Microsoft Defender for Cloud

1. Enable Microsoft Defender for Cloud.

6.4.10. Key Vault

1. Deploy and configure Azure Key Vault for secure storage of keys, certificates, and secrets.

6.4.11. Azure Backup

1. Implement Azure Backup for App Services, databases, and storage accounts.

6.4.12. API Management

1. Deploy API Management to manage, publish, and secure APIs.

6.5. Scope of Work for Cloud Infrastructure Operation & Management :

To ensure the smooth running of the Subhadra Portal, the scope of work for Cloud Infrastructure Operation & Management includes the following key areas:

1. **Performance Monitoring and Optimization**:
    a. Continuously monitor the performance of cloud resources and applications.
    b. Track metrics and logs.
    c. Optimize resource usage to ensure efficient performance and cost management.
2. **Security and Compliance**:
    a. Implement robust security measures, including firewalls, encryption, and access controls.
3. **High Availability and Disaster Recovery**:
    a. Design and implement high availability architectures to minimize downtime.
    b. Develop and test disaster recovery plans to ensure data integrity and quick recovery.
4. **Automation and Orchestration**:
    a. Use automation tools to streamline repetitive tasks and orchestrate complex workflows.
    b. Implement CI/CD pipelines for continuous integration and deployment.
5. **Cost Management**:
    a. Monitor and manage cloud costs to avoid unnecessary expenses.
6. **User Support and Training**:
    a. Provide support and training to users to help them effectively utilize cloud resources.
    b. Develop documentation and conduct training sessions.
7. **Incident Management**:
    a. Implement a robust incident management process to quickly detect and resolve issues.

The Service Provider needs to ensure following compliance level for each of the Service Levels.

Table- Compliance Level for SLAs

The penalty against SLAs would be as follows:

Table-Penalty for SLAs

Parameter	Target	Basis	Penalty
Application Uptime* including ✓ Database Server Uptime ✓ Application Server Uptime ✓ Web Server Uptime ✓ All SAN Storage Uptime ✓ Internet Link ✓ Any other IT component in the Infrastructure Architecture	>= 99.99%	Per 0.5% breach of target. This will be calculated monthly after the Go-live of the application. Uptime (%) = $\frac{\text{hours application up in the month}}{\text{total hours in the month}} \times 100$	Per 0.5% breach of target penalty shall be Rs. 10,000. Maximum penalty of 5 % of quarterly payment amount. Penalty will be deducted from the quarterly payments.
• Application uptime refers to availability of application to end-users Downtime of services on holidays (national holidays and Sundays) or scheduled downtime will not be considered for calculation of compliance level and penalty. • Quarterly Penalty shall be deducted from Quarterly payment before making the payments.			

7. Bid Evaluation Criteria

7.1. Prequalification of CSP:

CSP should have following:

1. CSP should be a registered firm or a company in India and the proposed Data Centers (DC & DR) should have jurisdiction in India
2. Neither the current organization nor the holding company should have been Debarred and / or blacklisted by any organizations of Govt. of India/ Central PSU/ GoMP entities as on bid submission date
3. Proposed Cloud Service Provider (CSP) should be STQC audited and MeiTY empaneled and offer all services from India only as per guidelines of MeiTY
4. The Primary and DR Data Centre (Cloud) shall be physically located in India. The proposed Datacenter for DR should be at least 100 KM from current Primary Datacenter, and it should not be in same River Flood plain
5. The proposed data center must be Tier III or above for better availability of cloud services and certified under:
   a. TIA 942/ Uptime Institute Certification
   b. Data Centre should be either Seismic Zone-II or Seismic Zone-III only
6. CSP should have ISO-22301 certification.
7. CSP should be Visionary or Leader in Gartner Magic Quadrant for “Analytics and Business intelligence platform”.

8. CSP should be Visionary or Leader in Gartner Magic Quadrant for “Data science and Machine learning platforms”.
9. CSP should be a Leader in latest Gartner Magic Quadrant for “End Point Protection”.
10. CSP should be a Leader in latest Gartner Magic Quadrant for “Cloud Infrastructure as a Service”.
11. The CSP should provide financially backed SLAs for all the services offered and these SLAs should be declared in public portal of CSP.
12. The CSP should provide native marketplace with certified applications which can be deployed on cloud. The CSP should also provide capability for administrators to create private marketplace with images from the public marketplace.
13. The CSP should provide all variants of cloud service as per MeiTY guidelines.
    a. Infrastructure as a Service (IaaS),
    b. Platform as a Service (PaaS)
    c. Software as a Service (SaaS)
14. Cloud Service Providers must offer Cloud native turnkey SIEM offering to configure real-time analysis and alerting of security events. At a minimum, the integration or service must support alerting, log retention and some form of forensic analysis that is able to search across logs and periods of time for patterns.
15. CSP should have accreditations relevant to security, availability, confidentiality, processing integrity, and/or privacy Trust Services principles. SOC 1, SOC 2, SOC 3
16. Data Centers should be compliant at a minimum with the following:
    a. ISO 9001
    b. ISO/IEC 27001
    c. ISO/IEC 27017
    d. ISO/IEC 27018
    e. ISO/IEC 27701
    f. PCI DSS Level 1
17. Native Platform Services: proposed CSP should have native capabilities for the services below:
    a. CSP Managed Video Calling service
    b. CSP Managed Container Management Service
    c. CSP Managed Analytics Platform Services
    d. CSP Managed DevOps Services
    e. CSP Managed databases (PostgreSQL, MySQL & NoSQL)
    f. CSP Managed Generative AI services

7.2. Pre-qualification of Bidder

Sl#	Clause	Documents Required
1	The bidder must be registered under the Companies Act 1956 or a Partnership firm registered under LLP Act, 2008. The bidder must be registered under GSTN Odisha	• Certificate of incorporation • GST Identification number (GSTIN) • Income Tax registration/PAN number
2	The Bidder should have positive net worth during last three financial years, ending 31.03.2024	A certified document by the Chartered accountant stating the net worth and average annual turnover of the bidder.
3	The Bidder's average annual turnover should be more than (INR) 100 cores in last three financial years and profitable during each of the previous three financial years ending on 31.03.2024.	CA certificate along with Copy of audited profit and loss account/balance sheet/annual report of the last three financial year
4	The Bidder must have 10 cloud certified Engineer /Professionals on company payroll.	A self-certified letter by an authorized signatory mentioning the list of IT service engineer/professionals along with their EPF and valid OEM certificate of the person.
5	The Bidder shall not be under a Declaration of Ineligibility for corrupt or fraudulent practices or blacklisted with any of the Government.	Declaration in this regard by the authorized signatory of the Bidder
6	Bidder should have experience in Hosting & Maintenance of application/ website/ Portal on cloud	Purchase/Work Order copy with installation report/invoice/client letter should be submitted
7	Bidder should have single Purchase Order of ₹2.5 cr of any Cloud licenses /SAAS/managed Services	PO Copy to be submitted
8	Bidder should submit Authorization from OEM/CSP in the prescribed format for this project.	Tender specific authorization should be submitted.
9	Bidder should have ISO 9001, 20000-1, ISO 27001 & CMMI Level 3 or higher certificate	Valid copy of certificate to be submitted along with the PQ.
10	Bidder Should have single tenant with minimum consumption of Rs. 15 Lakhs per annum or more	Proof of relevant documents required
11	EMD amounting to ₹5,00,000/-	DD/BG
12	Pre-qualification of CSP	The bidder has to submit a copy of declaration duly signed by the OEM/CSP stating compliance to all the requirements stated in the "Pre-qualification of CSP"
13	Bidders' operation centre in Odisha	Trade License for operation in Odisha and lease agreement/ownership document. In case the bidder does not have an operation centre in Odisha, the bidder has to submit a declaration to open an operation centre within a month in case the bidder is selected in the bid.

7.3. Technical Evaluation Matrix

Sl#	Criteria	Max Mark	Document to be submitted
1	Avg Turnover of the bidder in last 3 FY should be: 100 Cr -15 marks For each additional 5 Crores -2.5 marks each	20	Balance sheet along with CA certified Avg Turnover certificate
2	Experience: One IT project value including Cloud Services/license in last 05 years. Project value of 3 Crore - 4 Marks for each 2 Crores -2 marks each	10	PO copy
3	Experience in Hosting, Maintenance and Management of application/ website/ Portal on cloud	10	PO copy
4	Bidder must have 10 cloud certified Engineer /Professionals on company payroll – 1 Marks each per certified engineer	10	A self-certified letter by an authorized signatory mentioning the list of IT service engineer/professionals along with their EPF and valid OEM certificate of the person.
5	Bidder Must have certification have ISO 9001: 2 Marks, ISO 20000-1: 2 Marks, ISO 27001: 2 Marks CMMI Level 3 certificate: 3 Marks CMMI Level 5 certificate: 4 Marks	10	Valid certificates
7	Bidder having office in Odisha :5 marks	5	Trade License for operation in Odisha and lease agreement/ownership document
		65 Marks	
8	Presentation on understanding Approach and methodology of the project	35	

Note – Bidder scoring more than 70 marks will qualify for financial bid evaluation.

7.4. Commercial Bid Evaluation

A detailed evaluation of the bids shall be carried out in order to determine whether the bidders are competent, enough and whether the technical aspects are substantially responsive to the requirements set forth in the RFP document. Bids received would be assigned scores based on the parameters defined in the table.

The bidder scoring more than 70 marks will qualify for financial bid evaluation.

The technically qualified bidders shall be invited during opening of the commercial bids and subsequently commercial evaluation shall be carried out.

The Evaluation Methodology proposed to be adopted by OCAC will be Quality cum Cost Based System (QCBS) method of evaluation where Technical Bid Score will get a weightage of 70% (denoted by ST) and Commercial Bid Score a weightage of 30% (denoted by SF).

The process of selection of successful bidder for the purpose of award of contract shall be as follow,

Calculation of Technical Score (ST)

T = Technical Marks Obtain by the Individual Bidder.

TH = Highest Technical Marks Obtain by bidder.

ST = Technical Score obtain by the Individual Bidder

Calculation of Technical Score (ST)

ST = 100 x (T/TH) (rounded off to 2 decimal places)

Calculation of Financial Score (SF)

F= Total Financial Bid amount quoted by individual Bidder

FL= Lowest Total Financial Bid amount quoted by individual Bidder.

SF = Financial Score obtain by the Individual Bidder

Calculation of Financial Score (SF)

SF = 100 x (FL/F) (rounded off to 2 decimal places).

Calculation of Final Composite Score (S)

The Final Composite Score (S) shall be computed for each firm by assigning 70% weightage to the Technical Score (ST) and 30% weightage to Financial Score (SF) using the formula given below:

S = (ST x 0.7) + (SF x 0.3) (rounded off to 2 decimal places)

Bidder with the highest final composite score will be awarded the contract. In case of a tie in the final composite score, the bidder with the higher Technical Score will be invited for negotiations and selection first.

All the bidders who will achieve 70 or more marks in the technical evaluation would be eligible for evaluation of their financial proposal.

8. Instruction to Bidders

1. Bidder should log into the website well in advance for the submission of the bid so that it gets uploaded well in time i.e. on or before the bid submission time. Bidder will be responsible for any delay due to other issues.
2. The bidder has to digitally sign and upload the required bid documents one by one as indicated in the tender document as a token of acceptance of the terms and conditions laid down by Department.
3. Bidder has to select the payment option as per the tender document to pay the tender fee / Tender Processing fee.
4. Bidders are requested to note that they should necessarily submit their financial bids in the format provided and no other format is acceptable. If the price bid has been given as a standard BOQ format with the tender document, then the same is to be downloaded and to be filled by all the bidders. Bidders are required to download the BOQ file, open it and complete cells with their respective financial quotes and other details (such as name of the bidder). No other cells should be changed. Once the details have been completed, the bidder should save it and submit it online, without changing

the filename. If the BOQ file is found to be modified by the bidder, the bid will be rejected.

5. Technically qualified bidders will be considered as successful bidders for price bid opening.
6. The bidder must submit all documents as asked in Annexure section.

8.1. Earnest Money Deposit (EMD)

1. Earnest Money Deposit (EMD) of ₹5,00,000/- (Rupees Five Lakhs only) in the form of Demand Draft, drawn from any Scheduled Bank in India, in favour of "Odisha Computer Application Centre", payable at Bhubaneswar or in shape of Bank guarantee valid for at least 6 months from the date of submission of bid.
2. The bid / proposal submitted without EMD, mentioned above, will be summarily rejected.

8.2. Completeness of the RFP Document

1. Submission of the RFP response shall be deemed to have been done after careful study of the RFP document with full understanding of its implications.
2. Failure to comply with the requirements or any clause of the RFP document may render non-compliant and the RFP Response may be rejected. Bidders must:
   a. Include all documentation specified in this RFP document;
   b. Follow the format prescribed in this RFP document and respond to each element in the order as set out in this RFP document.
   c. Comply with all requirements as set out within this RFP document.

8.3. Evaluation Criteria

1. OCAC may constitute an Evaluation Committee to evaluate the responses of the Bidders and all supporting documents/ Annexure as per the RFP document. Inability to submit requisite supporting documents or Annexure, may lead to rejection of the RFP Proposal. The Committee may seek additional documents as it deems necessary.
2. The decision of the Evaluation Committee in the evaluation of responses to the RFP shall be final. No correspondence will be entertained outside the evaluation process of the Committee.
3. The Evaluation Committee may ask for technical presentation from the Shortlisted Bidders in reference to the scope of work mentioned in this RFP.
4. The Commercial Bids of the qualified bidders will be evaluated based on the submitted artifacts/ annexure. After opening of financial bid, QCBS method will be used for selection of bidder.

9. General Terms & Conditions of Tender

9.1. General

The Purchaser is Odisha Computer Application Centre, OCAC Building, N-1/7-D, Acharya Vihar Square, Bhubaneswar – 751 013 Odisha.

9.2. Performance Bank Guarantee (PBG)

The Bidder shall furnish a **Performance Bank Guarantee (PBG) for 10% (ten percent)** of the contract price within 15 days of issue of Work Order by the purchaser. The PBG must be from the nationalized bank in India. This Performance Bank Guarantee (PBG) shall remain valid for 60 days beyond the entire contractual obligation. Failure of submission PBG within the specified time period may lead to cancel the Work Order.

9.3. Price

The Bidder shall quote price in clear terms. The rates quoted shall be per record of successful work and should abide by the Format for Financial Bid described in Annexure (P2): Price Bid. The rates quoted should be exclusive of Goods Service Tax or any other taxes/cess/duty imposed from time to time.

Prices quoted by the Bidder shall be fixed and no variation will be allowed under any circumstances. No open-ended bid shall be entertained and the same is liable to be rejected straightway.

Bids shall remain valid for 180 days after the date of bid opening prescribed by the OCAC. The OCAC holds the rights to reject a bid valid for a period shorter than 180 days as nonresponsive, without any correspondence.

9.4. Submission of Bid

The bid must be submitted in e-Nivida Portal (www.enivida.odisha.gov.in) before the last date and time of submission of bid

9.5. Project Timeline & Terms of Payment

The payment shall be in Indian Rupees and shall be paid as follows:

SL#	Description	Timeline	Payment Terms
1.	Provisioning of a) Data Centre & DR	Within 1 week from the issuance of LOI	Nil
2.	Migration of the application on the new Cloud environment (if any)	Within 2 weeks after provisioning the services as mentioned in Sr.No.1	Nil
3.	Operational Acceptance (OA)	1 week after provisioning both the services as mentioned in Sr.No.1&2	Nil
4.	Operation and Maintenance phase	Will start from the date of OA provided by OCAC.	Quarterly

The successful Bidder has to sign an agreement on non-judicial stamp paper.

9.6. Termination of Contract

1. Termination for Default

The OCAC may, without prejudice, to any other remedy for breach of contract, by written notice of default sent to the qualified Bidder, terminate the contract in whole or in part if:

a. The qualified Bidder fails to deliver any or all of the obligations within the time period(s) specified in the contract or any extension thereof granted by the OCAC.

b. The qualified Bidder fails to perform any other obligation(s) under the contract. However, the disputes if any may be referred to Arbitration.

2. Termination for Insolvency, Dissolution etc.

OCAC may at any time terminate the contract by giving written notice to the qualified Bidder without compensation to the qualified Bidder, if the qualified Bidder becomes bankrupt or otherwise insolvent or in case of dissolution of firm or winding up of company, provided that such termination will not prejudice or effect any right of action or remedy which has accrued thereafter to the OCAC.

The Purchaser shall have the option to terminate the contract, in whole or in part by giving at least 90 days' prior notice in writing. The Bidder shall, immediately upon receipt of such notice, take all reasonably necessary steps to bring the Services to a close in a prompt and orderly manner and shall make every reasonable effort to keep expenditures for this purpose to a minimum.

Without prejudice to the generality of the foregoing, the Purchaser will also be entitled to terminate the contract, if the Bidder breaches any of its obligations set forth in the contract and such breach is not cured within thirty (30) Working Days after the Purchaser gives written notice; or If such breach is not of the type that could be cured within thirty (30) Working Days, failure by Bidder to provide the Purchaser, within thirty (30) Working Days, with a reasonable plan to cure such breach, which is acceptable to the Purchaser.

The Bidder shall not have any right to terminate the contract for convenience.

The Bidder understands the largeness of this Project and that it would require tremendous commitment of financial and technical resources for the same from the Bidder for the tenure of this contract. The Parties therefore agree and undertake that if at any time after expiry of initial period of one year and during the terms of any subsequent renewal of this agreement, it is assessed by the Purchaser that the scope, size and technicalities of the Project has become such that its smooth execution could not be achieved and ensured by the Bidder then the Purchaser will have option of exit at any point. However, exit would happen only after the completion of the notice period of 90 days, and only after completion of the Bidder's obligations under a reverse transition mechanism. During this period of Reverse Transition, the Bidder will have to continue to provide the Deliverables and the Services in accordance with this contract and will have to maintain the agreed Service levels.

Immediately upon the date of expiration or termination of the contract, The Purchaser shall have no further obligation to pay any fees for any periods commencing on or after such date and shall be free to hire any other vendors found suitable for handling the project.

Upon the termination or expiry of this contract: The rights granted to the Bidder shall immediately terminate. Upon the Purchaser request, with respect to, (i) any agreements for maintenance, services or other third-party services used by the Bidder to provide the Services; and (ii) the assignable agreements, the Bidder shall, use its reasonable

commercial endeavours to assign such agreements to the Purchaser and its designee(s) till alternative arrangements are made by the Purchaser in that regard.

Upon the Purchaser request in writing, the Bidder will be under an obligation to transfer to the Purchaser or its designee(s) the Deliverables created by the Bidder for the Purchaser under this Agreement, free and clear of all liens, security interests, or other encumbrances at the contracted rates.

9.7. Payment upon Termination

In the event of a pre-mature termination of this Contract by the Purchaser, the compensation payable to successful Bidder will be decided in accordance with the Terms of Payment Schedule and the payment to the successful Bidder will be settled within 30 days of the termination of the contract.

In the event of such termination, the successful Bidder on transit period will work to transfer all the work completed and in progress and knowledge out of the project as per the requirement of the Purchaser.

9.8. No breach of Agreement

The failure of a Party to fulfil any of its obligations hereunder shall not be considered to be a breach of, or default under, the Contract insofar as such inability arises from an event of Force Majeure, provided that the Party affected by such an event has taken all reasonable precautions, due care and reasonable alternative measures, all with the objective of carrying out the terms and conditions of the Contract.

9.9. Delay, Penalty and Termination

Bidder shall not be liable for forfeiture of its performance security, liquidated damages or termination for default, if and to the extent that it's delay in performance or other failure to perform its obligations under the contract/ order subsequent to the Contract is the result of an event of Force Majeure.

If a Force Majeure situation arises, Bidder shall promptly notify the Purchaser in writing of such conditions and the cause thereof within twenty calendar days. Unless otherwise directed by the Purchaser in writing, Bidder shall continue to perform its obligations as per the order placed subsequent to this agreement as far as it is reasonably practical, and shall seek all reasonable alternative means for performance not prevented by the Force Majeure event.

In such a case, the time for performance shall be extended by a period(s) not less than the duration of such delay. If the duration of delay continues beyond a period of **three months**, the Purchaser and the Bidder shall hold consultations with each other in an endeavour to find a solution to the problem.

In the event of the Force Majeure conditions continuing for a period of more than **three months** the parties shall discuss and arrive at a mutually acceptable arrangement.

9.10. Negotiation

It is absolutely essential for the bidders to quote the lowest price at the time of making the offer in their own interest. The Purchaser, however, will have the discretion to choose to enter into any price negotiations.

9.11. Conflict of Interest

The Bidder shall disclose to the Purchaser in writing, all actual and potential conflicts of interest that exist, arise or may arise (either for the Bidder or its team) in the course of performing the services as soon as it becomes aware of such a conflict. Bidder shall hold the Purchaser's interest paramount, without any consideration for future work, and strictly avoid conflict of interest with other assignments.

In the event of any question, dispute or difference arising under the agreement or in connection there-with, the same shall be referred to the sole arbitration of the CEO, OCAC "the Purchaser" or in case his designation is changed or his office is abolished, then in such cases to the sole arbitration of the officer for the time being entrusted (whether in addition to his own duties or otherwise) with the functions of the CEO, OCAC "the Purchaser" or by whatever designation such an officer may be called (hereinafter referred to as the said officer), and if the CEO, OCAC "the Purchaser" or the said officer is unable or unwilling to act as such, then to the sole arbitration of some other person appointed by the CEO, OCAC "the Purchaser" or the said officer. The agreement to appoint an arbitrator will be in accordance with the Arbitration and Conciliation Act 1996. There will be no objection to any such appointment on the ground that the arbitrator is a Government Servant or that he has to deal with the matter to which the agreement relates or that in the course of his duties as a Government Servant he has expressed his views on all or any of the matters in dispute. The award of the arbitrator shall be final and binding on both the parties to the agreement. In the event of such an arbitrator to whom the matter is originally referred, being transferred or vacating his office or being unable to act for any reason whatsoever, the CEO, OCAC "the Purchaser" or the said officer shall appoint another person to act as an arbitrator in accordance with terms of the agreement and the person so appointed shall be entitled to proceed from the stage at which it was left out by his predecessors.

The arbitrator may from time to time with the consent of both the parties enlarge the time frame for making and publishing the award. Subject to the aforesaid, arbitration and Conciliation Act, 1996 and the rules made there under, any modification thereof for the time being in force shall be deemed to apply to the arbitration proceeding under this clause.

The venue of the arbitration proceeding shall be the office of the CEO, OCAC "the Purchaser", or such other places as the arbitrator may decide.

9.12. Data Ownership

All the data created as the part of the project shall be owned by the purchaser. The Bidder shall take utmost care in maintaining security, confidentiality and backup of this data. The purchaser shall retain ownership of any user created/loaded data and applications hosted

on Bidder's infrastructure and maintains the right to request (or should be able to retrieve) full copies of these at any time.

9.13. Fraud and Corruption

The Purchaser requires that Bidder must observe the highest standards of ethics during the execution of the contract. In pursuance of this RFP, the Purchaser defines, for the purpose of this provision, the terms set forth as follows:

1. "Corrupt practice" means the offering, giving, receiving or soliciting of anything of value to influence the action of the Purchaser in contract executions.
2. "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 practice among bidders (prior to or after bid submission) designed to establish bid prices at artificially high or non-competitive levels and to deprive The Purchaser of the benefits of free and open competition.
3. "Undesirable practice" means (i) establishing contact with any person connected with or employed or engaged by The Purchaser with the objective of canvassing, lobbying or in any manner influencing or attempting to influence the Selection Process; or (ii) having a Conflict of Interest; and
4. "Restrictive practice" means forming a cartel or arriving at any understanding or arrangement among Bidders with the objective of restricting or manipulating a full and fair competition in the Selection Process.
5. "Coercive Practices" means harming or threatening to harm, directly or indirectly, persons or their property to influence their participation in the execution of contract.
6. If it is noticed that the Bidder has indulged into the Corrupt / Fraudulent / Undesirable / Coercive practices (as be decided by a court or competent authority with appropriate jurisdiction), it will be a sufficient ground for The Purchaser for termination of the contract and initiate black-listing of the vendor.

9.14. Exit Management

1. Exit Management Purpose

This clause sets out the provisions, which will apply during Exit Management period. The Parties shall ensure that their respective associated entities carry out their respective obligations set out in this Exit Management Clause.

The exit management period starts, in case of expiry of contract, at least 3 months prior to the date when the contract comes to an end or in case of termination of contract, on the date when the notice of termination is sent to the Bidder. The exit management period ends on the date agreed upon by the Purchaser or Three months after the beginning of the exit management period, whichever is earlier.

2. Confidential Information, Security and Data

Bidder will promptly, on the commencement of the exit management period, supply to the Purchaser or its nominated agencies the following:

a. Information relating to the current services rendered and performance data relating to the performance of the services; documentation relating to the project, project's customized source code; any other data and confidential information created as part of or is related to this project;
b. Project data as is reasonably required for purposes of the project or for transitioning of the services to its replacing successful Bidder in a readily available format.
c. All other information (including but not limited to documents, records and agreements) relating to the services reasonably necessary to enable the Purchaser and its nominated agencies, or it's replacing vendor to carry out due diligence in order to transition the provision of the Services to the Purchaser or its nominated agencies, or its replacing vendor (as the case may be).
d. The Bidder shall retain all of the above information with them for 30 days after the termination of the contract, post which the provider has to wipe/purge/delete all information created or retained as part of this project.
e. Bidder will sign a Non-Disclosure Agreement with The Purchaser. The format for the same has been included in Annexure.

3. Employees

Promptly on reasonable request at any time during the exit management period, the Bidder shall, subject to applicable laws, restraints and regulations (including in particular those relating to privacy) provide to the Purchaser a list of all employees (with job titles and communication address) of the Bidder, dedicated to providing the services at the commencement of the exit management period; To the extent that any Transfer Regulation does not apply to any employee of the successful Bidder, the Purchaser or Replacing Vendor may make an offer of contract for services to such employee of the Successful Bidder and the Successful Bidder shall not enforce or impose any contractual provision that would prevent any such employee from being hired by the Purchaser or any Replacing Vendor.

4. Rights of Access to Information

At any time during the exit management period, the Bidder will be obliged to provide an access of information to the Purchaser and / or any Replacing Vendor in order to make an inventory of the Assets (including hardware / Software / Active / passive), documentations, manuals, catalogues, archive data, Live data, policy documents or any other material related to implementation of IT Infrastructure Solution for the Purchaser.

5. Exit Management Plan

Bidder shall provide the Purchaser with a recommended "Exit Management Plan" within 90 days of signing of the contract, which shall deal with at least the following aspects of exit management in relation to the SLA as a whole and in relation to the Project Implementation, the Operation and Management SLA and Scope of work definition.

a) A detailed program of the transfer process that could be used in conjunction with a Replacement Vendor including details of the means to be used to ensure continuing

provision of the services throughout the transfer process or until the cessation of the services and of the management structure to be used during the transfer;

b) Plans for the communication with such of the Bidder, staff, suppliers, customers and any related third party as are necessary to avoid any material detrimental impact on Project's operations as a result of undertaking the transfer;
c) Plans for provision of contingent support to the implementation of IT Infrastructure solution for a reasonable period (minimum one month) after transfer.
d) Exit Management Plan shall be presented by the Bidder to and approved by the Purchaser or its nominated agencies.
e) The terms of payment as stated in the Terms of Payment Schedule include the costs of the Bidder complying with its obligations under this Schedule.
f) During the exit management period, the Bidder shall use its best efforts to deliver the services.
g) Payments during the Exit Management period shall be made in accordance with the Terms of Payment Schedule with subsequent approval by the Technical Committee by the Purchaser.

9.15. Arithmetic errors correction

Arithmetic errors, if any, in the price break-up format will be rectified on the following basis:

1) If there is discrepancy in the price quoted in figures and words, the price, in figures or in words, as the case may be, which corresponds to the total bid price for the item shall be taken as correct.
2) It the Bidder has not worked out the total bid price or the total bid price does not correspond to the unit price quoted either in words or figures, the unit price quoted in words shall be taken as correct.

9.16. Language of Bids

The Bids prepared by the Bidder and all correspondence and documents relating to the Bids exchanged by the Bidder and the Purchaser, shall be written in the English Language only.

9.17. Force Majeure Condition

If the execution of the contract is delayed beyond the period stipulated in the consultancy as result of outbreak of hostilities, declaration of an embargo or blockade of fire, flood, acts of God, then Purchaser may allow such additional time by extending the time frame as considered to be justified by the circumstances of the case and its decision will be final. If additional time is granted by the Purchaser, the supply order shall be read and understood as if it had contained from its inception the execution date as extended.

9.18. Modifications & Withdrawal

The bid submitted may be withdrawn or resubmitted before the expiry of the last date of submission by making a request in writing to the competent authority of Purchaser to this

effect. No Bidder shall be allowed to withdraw the bid after the deadline for submission of bids.

9.19. Right to Reject/Accept the Tender

The purchaser reserves the right either to reject or accept any or all tenders. The purchaser has exclusive right to alter the quantities of materials at the time of placing the final purchase order. The type and quantity of items indicated in the tender are provisional and may change as per the actual requirement. After placing the purchase order, the purchaser may order to defer the delivery of the material. It may be clearly understood by the bidders that the purchaser need not assign any reason for the above action.

9.20. Patent Rights etc.

The vendor shall indemnify the purchaser against all claims, actions, suits and proceedings for the infringement or alleged infringement of any patent, design or copy write protected either in the country of origin or in India by use of any equipment supplied by the vendor claims if made on the purchaser, shall be notified to the vendor of the same and the vendor shall at his own expense either settled such dispute or conduct any litigation that may arise there from.

9.21. Jurisdiction of High Court of Odisha

Suites, if any arising out of the contract shall be filed by either party in a court of Law to which the jurisdiction of the High Court of Odisha extends.

9.22. Confidentiality

1. The Bidder shall not, and without the Purchaser prior written consent, disclose the contract or any provision thereof, or any specification, plan, Data, Application /Application design document/other artefacts or information furnished by or on behalf of the Purchaser in connection therewith to any person other than a person employed by the Bidder in the performance of the contract. Disclosure to any such employed person shall be made in confidence and shall extend only as far as may be necessary for purposes of such performance.
2. The Bidder shall not without the Purchaser prior written consent, make use of any document or information.
3. Any document other than the contract itself shall remain the property of the Purchaser and shall be returned (in all copies) to the Purchaser on completion of the Bidder’s performance under the contract if so required by the Purchaser.

9.23. Obligation to Carry out Purchaser's Instructions

The Bidder shall also satisfy the purchaser or this inspector that adequate provision has been made to carry out his instructions fully and with prompt attitude.

9.24. Indemnity

The Bidder shall indemnify the Purchaser from and against any costs, loss, damages, expense, claims including those from third parties or liabilities of any kind howsoever suffered, arising or incurred inter alia during and after the Contract period out of:

a) Any negligence or wrongful act or omission by the Bidder or any MSP with Bidder in connection with or incidental to this Contract or;
b) Any breach of any of the terms of this Contract by the Bidder, the Bidder's Team or MSP,
c) Any infringement of patent, trademark/copyright arising from the use of the supplied goods and related services or any party thereof

The Bidder shall also indemnify the Purchaser against any privilege, claim or assertion made by a third party with respect to right or interest in, service provided as mentioned in any Intellectual Property Rights and licenses.

9.25. Limitation of Liability towards the Purchaser

1. Neither Party shall be liable to the other Party for any indirect or consequential loss or damage (including loss of revenue and profits) arising out of or relating to the Contract.
2. Except in the case of Gross Negligence or Wilful Misconduct on the part of the Bidder or on the part of any person acting on behalf of the Bidder executing the work or in carrying out the Services, the Bidder, with respect to damage caused by the Bidder including to property and/or assets of the Purchaser or of any of Purchaser's vendors shall regardless of anything contained herein, not be liable for any direct loss or damage that exceeds (A) the Contract Value or (B) the proceeds the bidder may be entitled to receive from any insurance maintained by the Bidder to cover such a liability, whichever of (A) or (B) is higher For the purposes of this Clause, "Gross Negligence" means any act or failure to act by a Party which was in reckless disregard of or gross indifference to the obligations of the Party under the Contract and which causes harmful consequences to life, personal safety or real property of the other Party which such Party knew, or would have known if it was acting as a reasonable person, would result from such act or failure to act.
3. Notwithstanding the foregoing, Gross Negligence shall not include any action taken in good faith for the safeguard of life or property. "Wilful Misconduct" means an intentional disregard of any provision of this Contract which a Party knew or should have known if it was acting as a reasonable person, would result in harmful consequences to life, personal safety or real property of the other Party but shall not include any error of judgment or mistake made in good faith.
4. This limitation of liability slated in this Clause, shall not affect the Bidder's liability, if any, for direct damage by Bidder to a Third Party's real property, tangible personal property or bodily injury or death caused by the Bidder or any person acting on behalf of the Bidder in executing the work or in carrying out the Services.

9.26. Changes of Orders

1. The Purchaser may at any time, by written order given to the Bidder, make changes within the general scope of the Contract.
2. If any such change causes an increase or decrease in the cost of, or the time required for, the Bidder's performance of any provisions under the Contract, an equitable adjustment shall be made in the Contract Value or delivery schedule, or both, and the Contract shall accordingly be amended. Any claims by the Bidder for adjustment under this Clause must be asserted within fifteen (15) days from the date of the Bidder's receipt of Purchaser's Change Order.
3. Procedure of Change Orders
    a. Upon receiving any revised requirement/advice, in writing, from the Purchaser, the Bidder would discuss the matter with the Purchaser.
    b. In case such requirement arises from the side of the Bidder, it would communicate in writing the matter with Purchaser as well as discuss the matter, giving reasons thereof.
    c. In either of the two cases as explained in Clause (a) and Clause (b) above, both the parties will discuss on the revised requirement for better understanding and to mutually decide whether such requirement constitutes a Change Order or not.
    d. If it is mutually agreed that such requirement constitutes a "Change Order" then the Bidder will study the revised requirement and assess subsequent schedule and cost effect, if any.
    e. If Purchaser accepts the implementation of the Change Order in writing, then the Bidder shall commence to proceed with the enforcement of the Change Order.
    f. In case, mutual Agreement under Clause (d) above, i.e. whether new requirement constitutes the Change Order or not, is not reached, then the Bidder in the interest of the works, shall continue providing Services as defined under the Contract. The time and cost effects in such a case shall be mutually verified and recorded. Should it establish that the said work constitutes a Change Order, the same shall be compensated taking into account the records kept in accordance with the Contract.
    g. The Bidder shall submit necessary back up documents for the Change Order showing the break-up of the various elements constituting the Change Order for the Purchaser's review. If no Agreement is reached between the Purchaser and Selected Agency within 30 days after Purchaser's instruction in writing to carry out the change concerning all matters described above, either party may refer the dispute to the ' Technical Committee' comprising of senior officials from the Purchaser.

9.27. Term and Extension of the Period

1. The term under this Contract will be for a period of 15 months which shall start from day of signing of the Contract.
2. If required by the Purchaser, an extension of the term can be granted to the Bidders. The final decision will be taken by the Purchaser.

3. The Purchaser shall reserve the sole right to grant any extension to the term above mentioned and shall notify in writing to the Selected Agency, at least 1 month before the expiration of the term hereof, whether it will grant the Bidder an extension of the term. The decision to grant or refuse the extension shall be at the Purchaser's discretion.
4. Where the Purchaser is of the view that no further extension of the term be granted to the Bidder, the Purchaser shall notify the Bidder of its decision at least 1 (One) month prior to the expiry of the Term. Upon receipt of such notice, the Bidder shall continue to perform all its obligations hereunder, until such reasonable time beyond the term of the Contract with the Purchaser.

9.28. Obligation to Carry out Purchaser's Instructions

The Bidder shall also satisfy the purchaser or this inspector that adequate provision has been made to carry out his instructions fully and with prompt attitude.

9.29. Resolution of Disputes between the Purchaser and engaged Bidder

1. The Purchaser and the Bidder shall make every effort to resolve amicably by direct informal negotiation on any disagreement or dispute arising between them under or in connection with the Contract.
2. If, after thirty (30) days from the commencement of such informal negotiations, the Purchaser and the Bidder have been unable to resolve amicably a Contract dispute, the dispute should be referred to the Chief Executive Officer, OCAC for resolution.
3. If, after thirty (30) days from the commencement of such reference, Chief Executive Officer, OCAC have been unable to resolve amicably a Contract dispute between the Purchaser and the Bidder, either party may require that the dispute be referred to the Special Secretary to Govt., E&IT Department, Govt. of Odisha.
4. Any dispute or difference whatsoever arising between the parties (Purchaser and Bidder) to the Contract out of or relating to the construction, meaning, scope, operation or effect of the Contract or the validity of the breach thereof, which cannot be resolved through the process specified above, shall be referred to a sole Arbitrator to be appointed by mutual consent of both the parties herein. In the event the parties cannot agree to sole arbitrator, such arbitrator shall be appointed in accordance with the Indian Arbitration and Conciliation Act, 1996.

9.30. Documents prepared by the Bidder to be the Property of the "OCAC"

All plans, specifications, designs, reports, and other documents prepared by the bidder for the "the Purchaser" under this Contract shall become and remain the property of the "the Purchaser", and the Bidder shall, not later than upon termination or expiration of this Contract, deliver all such documents to the "the Purchaser", together with a detailed inventory thereof. The Bidder may retain a copy of such documents, but shall not use anywhere, without taking permission, in writing, from the Purchaser and the Purchaser reserves right to grant or deny any such request. If license agreements are necessary or

appropriate between the Bidder and third parties for purposes of development of any such computer programs, the Bidder shall obtain the Purchaser prior written approval to such agreements, and the “the Purchaser” shall be entitled at its. Discretion to require recovering the expenses related to the development of the program.

10. Annexure(s) - Bid Formats

10.1. Annexure (T1): General Information of Bidder

(To be submitted on Lead Bidder's company letter head)

1.	Name of the Company/Firm/Agency		
2.	Year Established		
3.	Address of Registered office		
4.	Address of Head Quarter		
5.	Telephone No (business)		
6.	Fax No (business)		
7.	Email Address (business)		
8.	Website		
9.	Name of the Managing Director/CEO		
10.	PAN No		
11.	Goods Service Tax Regd. No		
12.	No of full-time personnel (Technical in the Similar Domain) currently under employment		
13.	No. of years of proven experience of providing similar services		
14.	Quality Certification (ISO, CMMi, Etc.)		
15.	Annual turnover Audited Annual Turnover in last three years	Annual turnover of the in Rs.	
		FY	Turnover (Rs.)
		2021-22	
		2022-23	
		2023-24	

Signature of the Bidder
Date:
Place:

Company Seal

10.2. Annexure (T2): Self Declaration

(To be submitted on Lead Bidder's company letter head)

Date : _____

Ref/RFP: _____

To

GENERAL MANAGER (ADMN)
ODISHA COMPUTER APPLICATION CENTER
OCAC BUILDING, PLOT NO. N1/7-D,
RRL POST OFFICE, BHUBANESWAR-751 013

Sir

In response to the RFP No._____, Dt: _____. Ms. /Mr. _____, as a _____, I / We hereby declare that our company _____is having unblemished past record and was not declare ineligible for corrupt & fraudulent practices either indefinitely or for a particular period of time.

Signature of witness
Date:
Place:
Company Seal

Signature of the Bidder
Date:
Place:

10.3. Annexure (T3): Acceptance of Terms & Conditions of Tender Documents

(To be submitted on Lead Bidder's company letter head)

Date:

To

GENERAL MANAGER (ADMN)
ODISHA COMPUTER APPLICATION CENTER
OCAC BUILDING, PLOT NO. N1/7-D,
RRL POST OFFICE, BHUBANESWAR-751 013

Sir,

I have carefully gone through the Terms & Conditions contained in the Tender No._____, regarding RFP Name < _____>.

I declare that all the provisions of this Tender 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.

Signature of witness
Date:
Place:
Company Seal

Signature of the Bidder
Date:
Place:

10.4. Annexure (T5): Representative Authorization Letter

(To be submitted on Lead Bidder's company letter head)

Date : _____

Ref/RFP: _____

To

GENERAL MANAGER (ADMN)
ODISHA COMPUTER APPLICATION CENTER
OCAC BUILDING, PLOT NO. N1/7-D,
RRL POST OFFICE, BHUBANESWAR-751 013

Ms. /Mr. _____ is hereby authorised to sign relevant documents on behalf of the company in dealing with invitation reference No._____, dtd: _____.

S/He is also authorised to attend meetings & submit technical & commercial information as may be required by you in the course of processing above said application.

Thanking you,
Authorised Signatory

_____
Representative Signature

_____
Signature attested
Company Seal

10.5. Annexure (T7): Statement of Deviations

(To be submitted on Lead Bidder's company letter head)

Request for Proposal for Empanelment of CSPs
(RFP No: _____Date_____)

Bidders are required to provide details of all deviations, comments and observations or suggestions in the following format with seal and signature. You are also requested to provide a reference of the page number, state the clarification point and the comment/ suggestion/ deviation that you propose as shown below.

The Purchaser may at its sole discretion accept or reject all or any of the deviations, however it may be noted that the acceptance or rejection of any deviation by the Purchaser will not entitle the bidder to submit a revised price bid.

Further, any deviation mentioned elsewhere in the response other than in this format shall not be considered as deviation by the Purchaser.

List of Deviations

#	**Clarification point as stated in the tender document**	**Page / Section Number in RFP**	**Comment/ Suggestion/ Deviation**
1			

Signature of the Bidder
Place & Date

Company Seal

10.6. Annexure (T8): Compliance Check List

RFP No: _____, Date: _____

Please check whether following have been enclosed.

Sl#	Enclosure description	Enclosed (Y/N)	Annexure/Attachment/ Page No./ Envelop No. of the enclosure
1.	Copy of Certificate of Incorporation of Company or Registration Firm		
2.	Copy Goods Service Tax Registration Certificate, Copy of PAN allotted		
3.	General Information		
4.	Self-Declaration that the bidder hasn't been blacklisted / performance issues by any Govt./PSU		
5.	Acceptance of Terms & Conditions Contained in The Tender Document		
6.	Representative Authorization Letter		
7.	Technical Compliance		
8.	Statement of Deviations		
9.	RFP Document Fee		
10.	EMD		

Signature of the Bidder
Place & Date

Company Seal

10.7. Annexure (P1): Price Bid Submission Form

(To be submitted on Lead Bidder's company letter head)

To

GENERAL MANAGER (ADMN)
ODISHA COMPUTER APPLICATION CENTER
OCAC BUILDING, PLOT NO. N1/7-D,
RRL POST OFFICE, BHUBANESWAR-751 013

Ref: RFP no <_____> *dated <dd/mm/yy>*

Subject: Submission of proposal in response to the RFP for "----------, RFP No_____.

Dear Sir,

We, the undersigned, offer to provide the consulting services for *<Insert title of assignment>* in accordance with your Tender dated <Insert Date> and our Technical Proposal. Our attached Financial Proposal for the sum of *<Insert amount(s) in words and figures>.* This amount is inclusive of taxes as listed at Annexure P2 (Summary of Costs for each category) attached.

Our Financial Proposal shall be binding upon us subject to the modifications resulting from Contract negotiations, up to expiration of the validity period of the Proposal.

We understand you are not bound to accept any Proposal you receive.
We remain,
Yours sincerely,

Authorized Signature [In full and initials]:
Name and Title of Signatory:

10.8. Annexure (P2): Price Bid

Subhadra Portal

SL#	Service category	Service type	Custom name	Region	Description	Qty	Unit	Unit Cost (Excl. Tax)	Total Cost (Excl. Tax)	Tax	Total Cost (Incl. Tax)
1.1	Compute	Virtual Machines	CI/CD VM	Central India	1 D4a v4 (4 vCPUs, 16 GB RAM), Linux; 1 managed disk – S6; Inter Region transfer type, 5 GB outbound data transfer from Central India to East Asia	1	No				
1.2	Compute	Virtual Machines		Central India	D64s v4 (64 vCPUs, 256 GB RAM) x 730 Hours (Pay as you go), Linux, (Pay as you go); managed disks – E30; Inter Region transfer type, 5 GB outbound data transfer from Central India to East Asia	9	No				
2.1	Storage	Storage Accounts	Document Store	Central India	Block Blob Storage, General Purpose V2, Flat Namespace, LRS Redundancy, Hot Access Tier, 100 TB Capacity, 1,000 x 10,000 Write operations, 1 x 10,000 List and Create Container Operations, 10,000 x 10,000 Read operations, 1 x 10,000 Other operations. 1,000 GB Data Retrieval, 1,000 GB Data Write, SFTP disabled	1	No				
2.2	Storage	Storage Accounts	Angular - Static Web Site	Central India	Block Blob Storage, General Purpose V2, Flat Namespace, LRS Redundancy, Hot Access Tier, 100 GB Capacity - Pay as you go, 100 x 10,000 Write operations, 1 x 10,000 List and Create Container	1	No				

					Operations, 1,000 x 10,000 Read operations, 1 x 10,000 Other operations. 1,000 GB Data Retrieval, 1,000 GB Data Write, SFTP disabled						
3.1	Networking	Azure Front Door	CDN + WAF + TLS + Geo		Azure Front Door Premium - Base instance included, 1 TB Data Transfer Out to Client, 100 GB Data Transfer In to Origin, 1000 x 10,0000 Requests	1	No				
3.2	Networking	Network Watcher	Network Monitoring	Central India	10 GB Network Logs Collected, 1000 Checks for Network Diagnostics, 10 Connection Metrics, 1 DNS or App Gateway Servers x 50 GB logs ingested, 1 GB logs collected for Traffic Analytics (Standard processing), 1 GB logs collected for Traffic Analytics (Accelerated processing)	1	No				
3.3	Networking	Bandwidth	Egress for External APi		Internet egress, 500 GB outbound data transfer from Central India routed via Microsoft Global Network	1	No				
3.4	Networking	Azure Firewall		Central India	Standard tier, 1 Logical firewall units, 50 TB Data processed	1	No				
3.5	Networking	VPN Gateway		Central India	VPN Gateways, Basic VPN tier, 10 S2S tunnels, 128 P2S connections, 0 GB, Inter-VNET outbound VPN gateway type	1	No				
3.6	Networking	Azure DDoS Protection		Central India	Network Protection, Protection for 100 resources	1	No				
3.7	Networking	Load Balancer		Central India	Standard Tier: 5 Rules, 1,000 GB Data Processed	3	No				
4.1	Security	Key Vault	Encryption Key Storage	Central India	Vault: 10,000 operations	1	No				

4.2	Security	Microsoft Defender for Cloud	CSPM	Central India	Microsoft Defender for Cloud Security Posture Management: 8 Billable Resources	1	No				
4.3	Security	Microsoft Defender for Cloud	Anti-Malware	Central India	Microsoft Defender for Cloud Workload Protection: 9 Plan 1 servers x 730 Hours, 1 PostgreSQL Instance, 2 Storage accounts x 730 Hours with, Defender for APIs – Plan 1 with 1 estimated API monthly transactions, 1 Key Vault(s)	1	No				
5.1	Databases	Azure Database for PostgreSQL	Database	Central India	Flexible Server Deployment, General Purpose Tier, 1 D16ads v5 (96 vCores) x 730 Hours (Pay as you go), Storage - Premium SSD v2, 6128 GiB Disk size, 2000 Additional IOPS, 1000 Additional throughput MBps, 3 TiB Additional Backup storage - LRS redundancy, with High Availability	1	No				
5.2	Databases	Azure Database for PostgreSQL	Read	Central India	Flexible Server Deployment, General Purpose Tier, 1 D96ads v5 (96 vCores) x 730 Hours (Pay as you go), Storage - Premium SSD v2, 6128 GiB Disk size, 2000 Additional IOPS, 1000 Additional throughput MBps, LRS redundancy, without High Availability	1	No				
5.3	Databases	Azure Cache for Redis		Central India	Enterprise tier: x1 scale factor (capacity 2) x 1 E5 instances x 730 Hours, Pay as you go, Software IP cost is included - Central India	1	No				
6.1	Developer tools	Azure DevOps	CI CD Pipeline		1 Basic + Test Plans license users, Paid tier - 1 Microsoft Hosted Pipeline(s), 1	1	No				

					Self Hosted Pipeline(s), 1 GB Artifacts, 1 GitHub Advanced Security committers						
6.2	DevOps	Azure Monitor	Monitoring and APM	Central India	Log analytics: Log Data Ingestion: 5 GB Daily Analytics logs ingested, 15 GB Daily Basic logs ingested, 1 months of Interactive Data Retention, 10000 Prometheus metrics per node, 30 seconds of Metric collection interval, 7 Dashboards, 50000 Data samples queried per dashboard, 25 promql alerting rules, 25 promql recording rules; Application Insights: 3 months Data retention, 5 Minutes Execution frequency, Executing for 1 month ; resources monitored X 1 metric time-series monitored per resource, 5 Minutes Log Signal frequency with log signals monitored and {2} time series per signal, 10 Additional events (in thousands)	1	No				
6.3	IP Addresses			Central India	Global (ARM), 5 Static IP Addresses X 730 Hours, 5 Public IP Prefixes X 730 Hours	1	No				
7.1	Management and governance	Azure Backup	VM Backup	Central India	Azure VMs, Standard Backup policy, 4 Instance(s) x 1 GB, LRS Redundancy, Low Average Daily Churn, 5,387 GB Average monthly backup data in Standard Tier, 313 GB Average monthly backup data in Archive Tier	1	No				

7.2	Management and governance	Azure Backup	DB Backup	Central India	Azure PostgreSQL Servers, 1 Instance(s) x 100 GB, LRS Redundancy, 1,533 GB Average monthly backup data in Standard Tier	1	No				
8.1	Postgresql Reporting				Power Platform for Reporting services with Power bI Licenses	1	No				
9.1	Azure Support				Professional direct Support from Azure per month	12	Man-Month				
10.1	Management and monitoring				24X7 Infra Management per shift cost of 8 hrs	12	Man-Month				
10.2	Management and monitoring				24X7 Information Security Management per shift cost of 8 hrs	12	Man-Month				
10.3	Management and monitoring				24X7 DB/Storage Management shift cost of 8 hrs	12	Man-Month				
11.1	Manpower				Azure certified Manpower	12	Man-Month				
12.1	Implementation				One time implementation cost for Infra & Security Setup	1	Lumpsum				
13.1	Other Services				Other Services	1	Lumpsum				
Sub-Total-1											

Other Government Scheme

Sl#	Service#	Description	Qty	Unit	Unit Cost (Excl. Tax)	Total Cost (Excl. Tax)	Tax	Total Cost (Incl. Tax)
1.1	Compute Services	Virtual Machines-DB Prod-(8 vCPUs, 16 GB RAM), Linux	1	No				
1.2		Virtual Machines-Machine Learning Prod (Tesla T4 GPU enabled (8 vCPUs, 56 GB RAM) , Linux	2	No				
1.3		Virtual Machines-Microservices Prod-(8 vCPUs, 16 GB RAM) , Linux	2	No				
1.4		Virtual Machines-Machine Learning Staging-(Tesla T4 GPU enabled (4 vCPUs, 28 GB RAM), Linux	1	No				

1.5		Virtual Machines-Db+Microservices Staging-(8 vCPUs, 16 GB RAM,Linux)	1	No				
2.1	Managed Disks Services	Managed Disks -OS Disks-128 GB SSD	10	No				
2.2		Managed Disks -DB Disks-500 GB SSD with 3000 IOPS per disk	10	No				
3.1	Azure Services	Azure OpenAI Service-Language Models, GPT-4-Turbo-128K, 25,000 x 1,000 input tokens, 15,000 x 1,000 output tokens	1	No				
3.2		Azure Firewall-Network Firewall NGFW	1	No				
3.3		Azure Front Door-Web Application Firewall	1	No				
3.4		Azure NAT Gateway-NAT Gateway 1 TB	1	No				
3.5		Azure Backup-Backup for VM	5	No				
3.6		Azure DNS-DNS Service	1	No				
3.7		Azure AI Translator, S1: Standard Translation with 1,000,000 translated characters	1	No				
3.8		Azure DDoS Protection-Static IP Address	1	No				
4.1	Additional services	Bandwidth-500 GB Internet eGRess	1	No				
4.2		Bandwidth-Virtual Network 1 TB	1	No				
4.3		Load Balancer	1	No				
4.4		Load Balancer	1	No				
4.5		Microsoft Defender for Cloud-EDR/AV for servers	5	No				
Sub-Total-2								

Cost Summary

Sl#	Description		Total Cost per Month (Excl. Tax)	Tax in ₹	Total Cost per Month (Incl. Tax)
A.	Cost for Cloud Hosting of Subhadra Scheme	Sub Total-1			
B.	Cost for Cloud Hosting of Other Government Scheme (Price Discovery Components)	Sub Total-2			
Grand Total					

Note:

- **The authority reserves the right to terminate any/all of the services with prior notice to the bidder. However, the price will remain valid for 1 year and 3 months from the date of the opening of commercial bid.**
- **The authority reserves the right to negotiate the rate against any of the items.**

- **The bid price will be exclusive of all taxes and levies and shall be in Indian Rupees.**
- **Errors & Rectification: 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. If there is a discrepancy between words and figures, the amount in words will prevail".**
- **Total Amount (Total Project cost) will be considered for commercial valuation.**
- **Payment of Taxes and Duties shall be made as per actual during the time of billing.**

10.9. Annexure (P3): Non-Disclosure Agreement

(Sample Format – To be executed on a non-judicial stamped paper of requisite value)

WHEREAS, we, _____, having Registered Office at _____, hereinafter referred to as the COMPANY, are agreeable to execute "**Request for Proposal for Empanelment of CSPs** " as per scope defined in the **RFP No :** _____ **dated** _____ for _____ (hereinafter referred to as the OCAC) and,

WHEREAS, the COMPANY understands that the information regarding the OCAC requirements/infrastructure related information shared by the OCAC in their Request for Proposal is confidential and/or proprietary to the OCAC, and

WHEREAS, the COMPANY understands that in the course of submission of the offer for the said RFP and/or in the aftermath thereof, it may be necessary that the COMPANY may perform certain jobs/duties on the OCAC's properties and/or have access to certain plans, documents, approvals, data or information of the OCAC;

NOW THEREFORE, in consideration of the foregoing, the COMPANY agrees to all of the following conditions, in order to induce the OCAC to grant the COMPANY specific access to the OCAC's property/information, etc.;

The COMPANY will not publish or disclose to others, nor use in any services that the COMPANY performs for others, any confidential or proprietary information belonging to the OCAC, unless the COMPANY has first obtained the OCAC's written authorization to do so;

The COMPANY agrees that information and other data shared by the OCAC or, prepared or produced by the COMPANY for the purpose of submitting the offer to the OCAC in response to the said RFP, will not be disclosed to during or subsequent to submission of the offer to the OCAC, to anyone outside the OCAC;

The COMPANY shall not, without the OCAC's written consent, disclose the contents of this Request for Proposal (Bid) or any provision thereof, or any specification, document, plan, pattern, sample or information (to be) furnished or shared by or on behalf of the OCAC in connection therewith, to any person(s) other than those employed/engaged by the COMPANY for the purpose of submitting the offer to the OCAC and/or for the performance of the Contract in the aftermath. Disclosure to any employed/ engaged person(s) shall be made in confidence and shall extend only so far as necessary for the purposes of such performance.

Signature & seal of the Bidder (Authorized Signatory)

Place & Date:

Company Seal

****End of Document***