Request for Proposal (RFP)

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

RFP No. OCAC-NEGP-INFRA-0006-2022/22044
Date. 14/07/2022

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.GEM.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. NO.	Information	Details
1	**RFP Number and Date**	
2	**RFP Document Fee (non-refundable)**	INR 11,200 (with 12% GST) in the favour of ODISHA COMPUTER APPLICATION CENTRE payable at BHUBANESWAR.
3	**Bid Security Declaration**	Bid Security Declaration to be submitted as per format
4	**Pre-Bid Meeting and Venue**	21/07/2022, 04:00 PM Odisha Computer Application Centre (OCAC) OCAC Building, Plot No.-N-1/7-D, Acharya Vihar Square, Bhubaneswar-751013 (INDIA)
5	**Release of Addendum / Corrigendum (if any)**	22/07/2022
6	**Last date for submission of Bid**	06/08/2022, 02:00 PM
7	**Opening of Pre-qualification & Technical Bid**	06/08/2022, 04:00 PM

8	**Contact Person for queries (email)**	osdc@ocac.in, sk.bhol@nic.in
9	**Addressee and Address at which proposal in response to RFP notice is to be submitted:**	The General Manager (Admn) Odisha Computer Application Centre (OCAC) OCAC Building, Plot No.-N-1/7-D, Acharya Vihar Square, RRL Post Office, Bhubaneswar-751013
10	**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 limited tender document containing the detailed terms & conditions from the website www.odisha.gov.in, www.ocac.in, www.gem.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 its existing services (both OCAC and other department's services/ applications) and upcoming department's as well as State PSUs services/ applications /websites /portal or any associated portal / website for the purpose which may arise out of the evolving requirement by the Purchaser.

The proposed cloud solution shall be scalable, extensible, highly configurable, secure and very responsive and shall support integration and interfacing with other software and solutions (existing legacy and acquired in future), developed or used by OCAC or State Departments or its Directorates / associate institutions and / or other stakeholders.

4.2. General Requirements

- Engaged MSP/ CSP ("*the Bidders"*) shall host, deploy and operationalize the IT System Solutions as decided by the OCAC /State Departments or its Directorates/ Agencies in close-coordination / collaboration with OCAC.
- CSP will have to take over the future Web Applications/ Websites/ Portal configurations, operations and its continuous improvement in a seamless manner within 7days maximum from the project kick-off date and ensure web / portal hosting, help desk facility and operation & maintenance support in an uninterrupted manner during and after the transition.

The DR/BCP setup configuration is required to be completed within 15days from the project kick-off date during which the portal shall continue to be in operation.

- New portal /web application to be setup in a primary DC and DR.
- Migration of portal/ web application from the existing hardware setup to new hardware setup for both primary and DR (if any).
- Resolve all technical issues/ queries faced by portal/ web application users.
- Send Daily status reports and Ad hoc reports as required by the Purchaser.
- Provide web portal/ application maintenance support 24X7X365 days.
- 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 periodic intervals of every 6 months.
- 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.), Internet Leased Lines with fail-over/ redundancy).
- 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 is 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.
- 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.
- The DC shall be physically located in India. The Bidder must provide self-certification in this regard.
- Ensure adequate Internet Bandwidth for all portals / websites /applications hosted in the DC with SLA for availability, accessibility, security and response time and latency. The bidder should propose DC own IP address and have multiple upstream providers so that if connectivity from either service provider goes down, redundancy is maintained.
- The Bidder shall provide the tool to monitor the infrastructure proposed comprising of resource utilization of all the servers, storage, network devices, bandwidth, and facility to monitor the private cloud environment using the same console as that of monitoring tool.
- Provide DC Operations and Management Services in 24x7x365 days throughout the contract period.
- Provide 9x6 (9 hrs. x 6 days) rapid customer support to users/ stakeholders *via* email and telephone. This would primarily involve support on integration issues, on-boarding the portal, data requirements etc. In case of emergency / exception Bidder may be required to extend support over and above this support window.
- OCAC and its appointed third-party auditors may visit the Bidder DC /BCP for auditing. The Bidder shall provide assistance and furnish the relevant information requested by the auditors.
- Content management of the website will be managed and monitored by the Bidder.
- No freeware software to be used unless authorised by OCAC and its associated TPAs.

- The selected bidder should provide a declaration of data and data backup being maintained must reside in India.

4.3. DC and DR site Infrastructure Technical Requirements

4.3.1. General Cloud Requirements

- OCAC intends to avail a managed private cloud preferably for hosting "the Portal and its applications" at the Bidder's DC/ BCP.
- The DC shall be at least an Uptime/ TIA 942 certified Tier-3 DC providing 99.982% services availability SLAs.
- The DC shall be well equipped with physical, logical, network and infrastructure security solutions, access protection systems including physical access control, and shall maintain the logs of the access.
- The DC shall be well equipped with intrusion detection & protection systems, firewalls, system management solutions & tools, back-up & restore solutions, monitoring tools, network load balancer for applicable servers and network layer security amongst others.
- The DC shall have ability to scale up or down the servers/ compute resources on-demand/ as desired without significant down time.
- The compute infrastructure shall include the virtual machines, operating systems, application servers, database server, anti-virus solutions and system management & back-up agents.

The IT infrastructure should be hosted on private cloud. The cloud should have following capabilities:

a) All the virtual machines should be auto scalable in terms of RAM and CPU.
b) The cloud platform should be enough intelligent to predict incoming load and assign resources to virtual machines dynamically without rebooting system.
c) Cloud platform should always allocate automatically resources against running load to handle sudden spikes.
d) The cloud platform should provide high availability across virtual machines so that even if any host goes down, all guest virtual machines should be migrated to another host automatically.
e) Cloud platform should support horizontal load balancing along with vertical
f) Cloud provider should give a dashboard of all virtual machines to monitor allocated and used resources by the portal application.
g) Cloud dashboard should allow generating reports for trend analysis of system usage.
h) OCAC team should be able to get the console access of any virtual machines if require.
i) There should be provision to generate historical reports of resources utilization.
j) There should be admin panel to create, delete, start, stop, and copy virtual machines.
k) There should be provision to take snapshots of machines so that working images of testing/quality machines can be taken.

Note – "The Portal" compute infrastructure needs to be monitored continuously for resource consumption and scaled up/out to meet the performance levels of the services and should be able to generate appropriate alerts in case of any fault in any of the device within data-centre.

4.3.2. Disaster Recovery Management and Business Continuity Plan

a) CSP would be responsible for Disaster Recovery Services so as to ensure business continuity of operations in the event of failure of primary DC and meet the RPO and RTO requirements.

b) RPO should be less than or equal to 15 minutes and RTO shall be less than or equal to 4 hours
c) However, during the change from Primary DC to DR or vice-versa (regular planned changes), there should not be any data loss.
d) There shall be asynchronous replication of data between Primary DC and DR and the CSP will be responsible for sizing and providing the DC-DR replication link so as to meet the RTO and the RPO requirements.
e) During normal operations, the Primary DC will serve the requests. The Disaster Recovery Site will not be performing any work but will remain on standby. During this period, the compute environment for the application in DR shall be available but with minimum possible compute resources required for a functional DR as per the solution offered. The application environment shall be installed and ready for use. DR Database Storage shall be replicated on an ongoing basis and shall be available in full (100% of the PDC) as per designed RTO/ RPO and replication strategy. The storage should be 100% of the capacity of the Primary Data Centre site. This requirement could be carried out manually subject to meeting RPO/ RTO requirements.
f) In the event of a site failover or switchover, DR site will take over the active role, and all requests should be routed through DR site. The pre-requisite to route request to DR should be articulated properly and shared by service provider.
g) Whenever there is failover from primary DC to secondary (DR), compute environment for the application at DR site shall be equivalent to DC including all the security features and components of DC, without the failover components. Development/test/quality environment will not be required at DR site.
h) The installed application instance and the database shall be usable and the same SLAs as DC shall be provided.
i) The bandwidth at the DR shall be scaled up to the level of Data Centre when DR is activated.
j) The CSP shall conduct live DR drill for two days at the interval of every six months of operation wherein the Primary DC has to be deactivated and complete operations shall be carried out from the DR Site. However, during the change from DC to DR or vice-versa (regular planned changes), there should not be any data loss. The pre-requisite of DR drill should be carried out by CSP and OCAC jointly. Certificate for DR drill should be submitted to OCAC for compliance.
k) The CSP shall clearly define the procedure for announcing DR based on the proposed DR solution. The CSP shall also clearly specify the situations in which disaster shall be announced along with the implications of disaster and the time frame required for migrating to DR. The CSP shall plan all the activities to be carried out during the Disaster Drill and issue a notice to the OCAC at least two weeks before such drill.
l) The disaster recovery plan needs to be provided by the service provider which needs to be updated half-yearly.
m) The service provider should offer dashboard to monitor RPO and RTO.
n) Any lag in data replication should be clearly visible in dashboard and alerts of same should be sent to respective authorities.

4.3.3. Penalty for breach in Disaster Recovery Management

Sl. No.	Parameter	Target	Penalty
1)	RTO	4 hours	Rs. 10,000 per additional hour of delay subject to a maximum delay of 10 hours.

Sl. No.	Parameter	Target	Penalty
2)	RPO	30 Minutes	Rs. 10,000 per additional block of 30 minutes subject to a maximum delay of 5 hours.
3)	Live Drill	To be conducted every 6 months Successful switch over and operation of application	Rs. 1000 for delay of each week, subject to a maximum of 5 weeks delay.

4.3.4. Cloud Service Provisioning Requirements

a) Service provider should enable the Purchaser to provision / change cloud resources from application programming interface (API).
b) The user admin portal should be accessible via secure method using SSL certificate.
c) The Purchaser should be able to take snapshot of virtual machines from provisioning portal.
d) The Purchaser should be able to size virtual machine and select require operating system when provisioning any virtual machines.
e) The Purchaser should be able to predict his billing of resources before provisioning any cloud resources.
f) The Purchaser should be able to set threshold of cloud resources of all types of scalability.
g) The Purchaser should be able to provision all additional storages required for cloud services.
h) The Purchaser should be able to provision any kind of resources either static or elastic resources.
i) The Purchaser should get list of all cloud resources from provisioning portal.
j) The Purchaser should be able to set the scaling parameters like in case of horizontal scaling,
    - The Purchaser should be able to set percentage / quantity of RAM consumption to trigger new virtual machines.
    - The Purchaser should be able to set percentage / quantity of CPU consumption to trigger new virtual machines.
    - The Purchaser should be able to set percentage / quantity of network bandwidth to trigger new virtual infrastructure.
k) The Purchaser should be able to set port on which horizontal scaling will work. Port refers to be service port (*such as port 80, 443*) which should not change in case of horizontal scaling.
l) The Purchaser should be able to set minimum and maximum number of virtual machines which will be automatically provisioned as part of horizontal scaling to handle spike in load.

4.3.5. Data Management

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

4.3.6. Operational Management

a) CSP should upgrade its hardware time to time to recent configuration to delivery expected performance for the Purchaser.
b) Investigate outages; perform appropriate corrective action to restore the hardware, operating system, and related tools.
c) CSP should manage their cloud infrastructure as per standard ITIL framework in order to deliver appropriate services to the Purchaser.
d) CSP should deliver cloud having method and system for real time detection of resource requirement and automatic adjustments.

4.3.7. Compatibility Requirements

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

4.3.8. Cloud Network Requirement

a) CSP must ensure that cloud virtual machine of the Purchaser is into separate network tenant and virtual LAN.
b) CSP must ensure that cloud virtual machines are having private IP network assigned to cloud VM.
c) CSP must ensure that all the cloud VMs are in same network segment (VLAN) even if they are spread across multi DC of CSP.
d) CSP should ensure that clouds VMs are having Internet and virtual network interface cards.
e) CSP should ensure that Internet vNIC card is having minimum 1 Gbps network connectivity and service vNIC card is on minimum 10 Gbps for better internal communication.
f) In case of scalability like horizontal scalability, the Service provider should ensure that additional requirement of network is provisioned automatically of same network segment.
g) CSP must ensure that public IP address of cloud VMs remains same even if cloud VM gets migrated to another DC due to any incident.
h) CSP must ensure that public IP address of cloud VMs remains same even if cloud VM network is being served from multiple CSP DC.
i) CSP must ensure that the public network provisioned for cloud VMs is redundant at every point.
j) CSP must ensure that clouds VMs are accessible from the Purchaser private network.
k) CSP must ensure that there is console access to cloud VMs, if the Purchaser requires accessing it.
l) CSP should ensure that cloud VM network is IPV6 enabled and all public facing devices are able to receive and transmit IPV6 data in addition to IPV4.
m) CSP should have provision of dedicated virtual links for data replication between their multiple DC in order to provide secure data replication for DR services.
n) CSP should ensure use of appropriate load balancers for network request distribution across multiple cloud VMs.

4.3.9. Cloud Storage Service Requirements

a) CSP should provide scalable, dynamic and redundant storage.

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

4.3.10. Portal Security

a) Tools for real time monitoring web site security Protection against defacement, hacking
b) Design should incorporate security features to protect the site from Session Hijacking, SQL injection, Cross scripting, Denial of Service (DDOS) etc.
c) Portal system should maintain a secure Password policy
d) Portal system should be secured by using Intrusion detection system (IDS) and Intrusion prevention system (IPS) at network level.
e) Attain security certification for the new website from CERT-IN through their empanelled vendors. CERT-IN security audit should be conducted every 6 months as per planned schedule.
f) Have current vulnerability assessments and PCI (Payment Card Industry) scanning performed for all the new modules being hosted on the Website / Portal.
g) The portal should be secured through a Web Application Firewall (WAF) as a service.
h) Bidder will have sole responsibility for fool proof security of the website / portal and need to provision all tools / real time monitoring to ensure the security of the website / portal.
i) Applications / Software Solutions shall comply with ISO 27001 Information Security Standard
j) Applications / Software Solutions and infrastructure shall have Authentication – Authorization – Access audit trails
k) Applications / Software Solutions shall be protected from security breaches, vulnerabilities such as:
    - SQL Injections
    - Script Injections
    - Cross Site Scripting
    - SSL Vulnerabilities
    - OWASP Vulnerabilities
    - And other vulnerabilities and security attacks.
l) All Service end-points- exposed over internet or internal shall be secured with at least 128 bits (desired 256 bits) SSL Certificates
m) All Servers, Services, Applications / Software Solutions shall have hardened security and reviewed regularly.
n) Any unauthorized access / attempt shall be reported immediately
o) The entire data-centre network shall have multiple levels of physical, logical, and network security systems for information protection including but not limited to IPSEC Policies, Firewalls, IDS / IPS protection Systems.
p) Portal and its security should be compliant with government of India guidelines issued from time to time.

4.3.11. Penalty for non-compliance of Portal Security Audit

CERT-IN Security Audit Certificate for the entire application and the action to be taken for compliance in every 6 months without failing. Non-compliance to the same shall be penalised and amount of Rs. 25,000/- shall be imposed on the CSP.

4.3.12. Cloud Security Requirements

a) CSP should ensure there is multi-tenant environment and cloud virtual resources of the Purchaser are logically separated from others.
b) CSP should ensure that any OS provisioned as part of cloud virtual machine should be patched with latest security patch.
c) In case, the CSP provides some of the System Software as a Service for the project, Service provider is responsible for securing, monitoring, and maintaining the System and any supporting software.
d) CSP should implement industry standard storage strategies and controls for securing data in the Storage Area Network so that clients are restricted to their allocated storage
e) CSP should deploy public facing services in a zone (DMZ) different from the application services. The Database nodes (RDBMS) should be in a separate zone with higher security layer.
f) CSP should give ability to create non-production environments and segregate (in a different VLAN) non-production environments from the production environment such that the users of the environments are in separate networks.
g) CSP should have built-in user-level controls and administrator logs for transparency and audit control.
h) CSP cloud platform should be protected by fully-managed Intrusion detection system using signature, protocol, and anomaly based inspection thus providing network intrusion detection monitoring.
i) CSP would be responsible for proactive monitoring and blocking against cyber-attacks and restoration of services in case of attacks.

4.3.13. Virtual Machine specifications

a) The Cloud virtual machine provided by CSP should be provisioned on redundant physical infrastructure.
b) The cloud virtual machines should be auto-scalable in terms of RAM and CPU with minimum downtime and should be able to give redundancy based on the way the VM's are provisioned.
c) The Purchaser should be able to provision cloud virtual machine of any operating system like Linux and Windows.
d) CSP should clearly define policies to handle data in transit and at rest.
e) Without handover of entire data back to the Purchaser, CSP should not delete any data at the end of contract period without consent from the Purchaser.
f) CSP should provide facility to make template from virtual machines.
g) CSP should make provision to add any virtual machine as part of scalable infrastructure.
h) CSP should have provision to live migration of virtual machine to another physical server in case of any failure.
i) CSP should deliver cloud having method and system for detecting, in real time, resource requirements of a system in virtual environment and automatic scaling of resource parameters to compensate resource requirement in a system. If a resource requirement is detected with any virtual machine, the automatic resource scaling system detects the type of resource to be scaled and scales the selected resource. Further, the resource may be scaled up or scaled down, based on the requirements. Further, the scaled resource may be CPU, RAM, disk or any such resource. The proposed system helps to save space and power without compromising security, performance and accessibility

4.3.14. Cloud resource and Network monitoring

a) CSP should give provision to monitor the network traffic of cloud virtual machine.

b) CSP should offer provision to analyse of amount of data transferred of each cloud virtual machine.
c) CSP should provide network information of cloud virtual resources.
d) CSP should offer provision to monitor latency to cloud virtual devices from its data centre or the Purchaser should be able to set monitoring of latency to cloud VMs from outside.
e) CSP must offer provision to monitor network uptime of each cloud virtual machine.
f) CSP must make provision of resource utilization i.e. CPU graphs of each cloud virtual machine.
g) CSP must make provision of resource utilization graph i.e. RAM of each cloud virtual machine. There should be provision to set alerts based on defined thresholds. There should be provision to configure different email addresses where alerts can be sent.
h) CSP must make provision of resource utilization graph i.e. disk of each cloud virtual machine. There should be graphs of each disk partition and email alerts should be sent if any threshold of disk partition utilization is reached.
i) CSP should give provision to monitor the uptime of cloud resources. The report should be in exportable form.
j) CSP must give provision to monitor the load of Linux/ Windows servers and set threshold for alerts.
k) CSP should make provision to monitor the running process of Linux/ Windows servers. This will help the Purchaser to take the snapshot of processes consuming resources.
l) CSP must ensure that there should be historical data of minimum 6 months for resource utilization in order to resolve any billing disputes if any.
m) CSP must ensure that audit logs of scalability i.e. horizontal and vertical is maintained so that billing disputes can be addressed.
n) CSP must ensure that log of reaching thresholds used to trigger additional resources in auto provisioning are maintained.
o) CSP must ensure that there are sufficient graphical reports of cloud resource utilization and available capacity.
p) CSP should provide network information of cloud virtual resources.
q) CSP should offer provision to monitor latency to cloud virtual devices from its DC or the Purchaser should be able to set monitoring of latency to cloud VMs from outside.
r) CSP must offer provision to monitor network uptime of each cloud virtual machine.
s) CSP must provide utilization reports for Internet bandwidth, load balancers etc.

4.3.15. Application Performance Monitoring (APM)

❖ **Database monitoring:**

1. APM should be able to provide overview of database server like Database details, version etc.
2. APM should be able to provide host details which are connected to database server
3. APM should be able to provide session details of all active database sessions.
4. Monitoring & management of network link proposed as part of this solution.
5. APM should be able to provide server configuration details (All configurations, Advanced Configurations, Reconfigure Configurations, and Memory Configurations)
6. Bandwidth utilization, latency, packet loss etc.
7. APM should be able to provide Jobs and Backup Details, including the following:
    - Currently executing Jobs
    - Job Steps Execution Information
    - Job Schedule Information
    - Recent Database Backup
    - Back-Up within Past 24 Hours

8. APM should monitor and provide details on the following queries performance parameters:
    - Top Queries by CPU , Top Queries by I/O
    - Top Waits by Waiting Tasks , Top Slow Running Queries
    - Most Frequently Executed Queries, Most Blocked Queries
    - Top Queries by Lowest Plan Reuse, Cost of Missing Indexes

9. APM should provide to set following monitoring parameters for continuous monitoring:
    - Total Server Memory, SQL Cache Memory
    - Optimizer Memory, Lock Memory
    - Connection Memory, Target Server Memory
    - Granted Work Space Memory, Buffer Cache Hit Ratio
    - Page Lookups/Sec, Pages Read/Sec
    - Page Life Expectancy (ms)
    - User Connections, Logins/Sec
    - Logouts/Sec, Cache Hit Ratio
    - Cache Count, Cache Pages
    - Lock Requests/Sec, Lock Wait/Sec
    - Lock Timeout/Sec , Full Scans/Sec
    - Range Scans/Sec, Probe Scans/Sec
    - Work Files Created/Sec, Work Tables Created/Sec
    - Index Searches/Sec, Latch Waits/Sec
    - Average Latch Wait Time, Batch Requests/Sec
    - SQL Compilations/Sec, SQL Recompilations/Sec
    - Auto-Param Attempts/sec, Failed Auto-Params/Sec
    - Safe Auto-Params/Sec, Unsafe Auto-Params/Sec
    - Availability

❖ Web Server:

1. APM should provide website details hosted on web server.
2. APM should provide application details running on web server.
3. Monitoring & management of network link proposed as part of this solution.
4. Bandwidth utilization, latency, packet loss etc.
5. APM should consist of the following monitoring parameters:
    - Site Status, Total Bytes Sent
    - Bytes Sent/Sec, Total Bytes Received
    - Bytes Received/Sec, Total Bytes Transferred
    - Bytes Total/Sec, Total Files Sent
    - Files Sent/Sec, Total Files Received
    - Files Received/Sec, Current Connections
    - Maximum Connections, Total Connection Attempts
    - Total Logon Attempts, Service Uptime

❖ Application / Web Server:

1. APM should consist of the following monitoring parameters:
    - Memory Monitoring
    - Web Applications and Deployments
    - Connections, Transactions, Queries
    - Web Metrics
    - Transactions
    - Availability

2. Monitoring & management of network link proposed as part of this solution.
3. Bandwidth utilization, latency, packet loss etc.

4.3.16. Backup Services

a) CSP must provide backup of cloud resources. Backups should be maintained at both off-site and on-site locations in secure fire proof and environmentally controlled environments so that the backup media are not harmed.
b) CSP should perform backup and restore management in coordination with the OCAC & procedures for backup and restore, including performance of daily, weekly, monthly, quarterly and annual backup functions (full volume and incremental) for data and software maintained on the servers and storage systems using Enterprise Backup Solution.
c) Backup and restoration of Operating System, application, databases and file system etc. in accordance with defined process / procedure / policy.
d) Monitoring and enhancement of the performance of scheduled backups, schedule regular testing of backups and ensure adherence to related retention policies
e) Ensuring prompt execution of on-demand backups & restoration of volumes, files and database applications whenever required.
f) Real-time monitoring, log maintenance and reporting of backup status on a regular basis. Prompt problem resolution in case of failures in the backup processes.
g) Media management including, but not limited to, tagging, cross-referencing, storing (both on-site and off-site), logging, testing, and vaulting in fire proof cabinets if applicable.
h) Generating and sharing backup reports periodically
i) Coordinating to retrieve off-site media in the event of any disaster recovery
j) Periodic Restoration Testing of the Backup
k) Maintenance log of backup/ restoration

4.3.17. Web Application Firewall (WAF) as Service

a) Cloud platform should provide Web Application Filter for OWASP (Open Web Application Security Project)
b) WAF should be able to support multiple website security.
c) WAF should be able to perform packet inspection on every request covering all 7 layers.
d) WAF should be able to block invalidated requests.
e) WAF should be able to block attacks before it is posted to website.
f) WAF should have manual control over IP/ Subnet. i.e., Allow or Deny IP/ Subnet from accessing website.
g) The attackers should receive custom response once they are blocked.
h) Must offer provision to customize response of vulnerable requests.
i) WAF should be able to monitor attack incidents and simultaneously control the attacker IP.
j) WAF should be able to Grey list or Backlist IP/ Subnet.
k) WAF should be able to set a limit to maximum number of simultaneous requests to the web server & should drop requests if the number of requests exceeds the threshold limit.
l) The WAF should be able to set a limit to maximum number of simultaneous connections per IP. And should ban / block the IP if the threshold is violated.
m) Should be able to set a limit to maximum length of path to URL.
n) Should be able to limit maximum size of request to Kilobytes.
o) WAF should be able to limit maximum time in seconds for a client to send its HTTP request.
p) Should be able to BAN an IP for a customizable specified amount of time if the HTTP request is too large.
q) Should be able to limit maximum size of PUT request entity in MB
r) The WAF should be able to close all the sessions of an IP if it is ban.

s) Should be able to Ban IP on every sort of attack detected and the time span for ban should be customizable. There should be a custom response for Ban IP.
t) The Dashboard should show a graphical representation of
    - Top 5 Attacked Websites.
    - Top 5 Attacking IP.
    - Top 5 Attack types.
    - Top 5 Attacked URLs.

u) For analysis purpose the Dashboard should contain following information:
    - Number of requests to web server.
    - Number of attacks.
    - Number of Attackers.
    - Types of error messages and error messages sent to the users.
    - Total Bytes sent during transaction

4.3.18. Malware Monitoring Services, Application Audit, External Vulnerability Assessment Service

a) Monitoring of Web Applications/ portals and protect it from malicious mobile codes like computer viruses, worms, Trojan horses, spyware, adware, key-loggers and other malicious programs. The service should be Non-Intrusive in nature and should be offered for at least 50 URLs.
b) Malware Monitoring scanning should be performed on Daily basis. If any malware is injected into Web Applications then immediate malware alert message is forwarded to the stake-holders. Application Audit and Vulnerability assessment on weekly basis to ascertain if any corrective action needs to be taken in application based on any observations found in the scanning.
c) Should be able to detect malicious code injection/ links, both known and unknown malware, Web-page tampering, various zero-day browser exploits etc.
d) Should be able to identify the malware source, malware threat area and coverage, encoded Java Script and VB script and should not rely on pattern/signature-based technology.
e) It should have minimal impact on traffic, server performance, networks etc. during deployment and operation
f) Should be able to work in any network topology.
g) Should be able to identify applications running on non-standard ports
h) Should have configurable scan intervals (frequency), Configurable notification, alerting and reporting options, Configurable “whitelist” option for allowed links, Configurable scan schedules and on-demand scans.
i) Should have Real-time instant alerting upon detection of malicious behaviour (Email or SMS).
j) Should have detailed remediation recommendation guidance including step by step instructions on how to address the threats captured
k) Should have On demand Vulnerability Scanning without user intervention
l) Should Perform a targeted scan (i.e. check for a specific set of vulnerabilities or IP Addresses).
m) Should be able to conduct vulnerability assessment for all operating systems and their versions including but not limited to: Windows, AIX, UNIX, Linux, Solaris servers etc.
n) Should be able to perform authenticated and unauthenticated scans
o) Should be able to detect weak password
p) Should be able to identify out-of-date software versions, applicable patches and system upgrades
q) Should Flag the presence of any blacklisted software

r) Should be able to perform on demand Application Audit for all types of websites including AJAX, WEB2.0, and obfuscated Java Script etc. and identifies vulnerabilities throughout the entire application, scanning the browser and server-side components.
s) Should check regularly for Defacement Detection, websites changes and detect for possible defacement. Such daily defacement checks protect the brand, credibility and reputation of the bank.
t) Should have an Executive Dashboard that provides a comprehensive synopsis of reported vulnerabilities and malware, remediation suggestions as well as several alert and support options in predefined report formats. It should have Role based access.
u) Should be able to provide remediation information in the reports including links to patches etc.
v) Should be able to produce a report listing all applications on a host or network, regardless of whether the application is vulnerable
w) Should include a library of potential vulnerabilities and rules which covers SANS (SANS Institute) top 20. This library should be customizable by administrator and changes to the same are to be traceable.
x) Should be able to produces reports preferably in the PDF format
y) Should be able to generate reports on trends in vulnerabilities on a particular asset
z) Should have Scan history and comparison provided in Scan Report
aa) Should have banner grabbing feature which tries to discover web-applications in the domain.
bb) Should Support industry standard reporting including OWASP top 10 categories
cc) Should support authenticated scanning with different authentication methods including Form, HTTP basic, NTLM and digest.
dd) The web application vulnerability scanning module should be able to identify the following vulnerabilities but not limited to in the underlying application

- XSS
- Form Validation
- Block Malformed content
- Back Doors
- Spoofing
- SQL injection
- Directory/path traversal
- Forceful browsing
- LDAP injection
- SSI injections
- XPath injection
- Sensitive information leakage

ee) Should be able to check mail server IP and check in multiple RBL repositories
ff) Should be able to scan SQL Injections for My SQL, MSSQL, PGSQL, Oracle databases.
gg) Should be able to scan Local file inclusion (LFI), Remote file inclusion (RFI), XSS - Cross Site Scripting & Malware.
hh) The scanning should support\cover following

- Open ports scanning for Security Threats
- Banner detection, directory scanning & directory indexing.
- Full Path disclosure in the pages
- Password auto complete enabled fields
- Page defacement detection & view state decoder
- Password submission method
- Time based scanning
- Robust link crawler
- SSL Certificate checking

- Web Shell Locater & Web Shell Finder
- Reverse IP domain check

4.3.19. Database Support Service

a) Installation, configuration, maintenance of the database (Cluster & Standalone).
b) Regular health check-up of databases.
c) Regular monitoring of CPU & Memory utilization of database server, Alert log monitoring & configuration of the alerts for errors.
d) Space monitoring for database table space, Index fragmentation monitoring and rebuilding.
e) Performance tuning of Databases.
f) Partition creation & management of database objects, Archiving of database objects on need basis.
g) Patching, upgrade & backup activity and restoring the database backup as per defined interval.
h) Schedule/ review the various backup and alert jobs.
i) Configuration, installation and maintenance of Automatic Storage Management (ASM), capacity planning/ sizing estimation of the Database setup have to be taken care by the Bidder.
j) Setup, maintain and monitor the 'Database replication' / Physical standby and Asses IT infrastructure up-gradation on need basis pertaining to databases.
k) Tuning of high cost SQLs and possible solution to application development team for tuning in order to achieve optimum database performance.

4.3.20. Managed Services

❖ **Network and Security Management:**

a) Monitoring & management of network link proposed as part of this solution.
b) Bandwidth utilization, latency, packet loss etc.
c) Call logging and co-ordination with vendors for restoration of links, if need arises.
d) Redesigning of network architecture as and when required by the Purchaser
e) Addressing the ongoing needs of security management including, but not limited to, monitoring of various devices / tools such as firewall, intrusion protection, content filtering and blocking, virus protection, and vulnerability protection through implementation of proper patches and rules.
f) Ensuring that patches / workarounds for identified vulnerabilities are patched / blocked immediately
g) Ensure a well-designed access management process, ensuring security of physical and digital assets, data and network security, backup and recovery etc.
h) Adding/ Changing network address translation rules of existing security policies on the firewall
i) Diagnosis and resolving problems related to firewall, IDS /IPS.
j) Managing configuration and security of Demilitarized Zone (DMZ) Alert / advice the Purchaser about any possible attack / hacking of services, unauthorized access / attempt by internal or external persons etc.

❖ **Server Administration and Management:**

a) Administrative support for user registration, User ID creation, maintaining user profiles, granting user access, authorization, user password support, and administrative support for print, file, and directory services.

b) Setting up and configuring servers and applications as per configuration documents/ guidelines provided by the Purchaser.
c) Installation/ re-installation of the server operating systems and operating system utilities
d) OS Administration including troubleshooting, hardening, patch/ upgrades deployment, BIOS & firmware upgrade as and when required/ necessary for Windows, Linux or any other O.S proposed as part of this solution whether mentioned in the RFP or any new deployment in future.
e) Ensure proper configuration of server parameters, operating systems administration, hardening and tuning
f) Regular backup of servers as per the backup & restoration policies stated by the Purchaser from time to time
g) Managing uptime of servers as per SLAs.
h) Preparation/ up-dation of the new and existing Standard Operating Procedure (SOP) documents on servers & applications deployment and hardening

❖ **Software Deployment on Hosting Infrastructure and Management:**

Support for deployment, testing, accessibility, load balancing, security management for all software deployed on the hosting infrastructure in coordination with the software development partner and the Purchaser (OCAC Team).

4.3.21. Helpdesk Support from Cloud Service Provider

a) CSP should provide flexibility of logging incident manually via web interface.
b) The web interface console of the incident tracking system would allow viewing, updating and closing of incident tickets
c) Allow categorization on the type of incident being logged
d) Provide classification to differentiate the criticality of the incident via the priority levels, severity levels and impact levels
e) Provide audit logs and reports to track the updating of each incident ticket
f) It should be able to log and escalate user based requests.
g) CSP should allow ticket logging by email, chat or telephone.
h) The Helpdesk Infra such as Toll Free number, ACD, etc. is required to be provided by the vendor.
i) Helpdesk support will be limited to DC & Application support only, End User Support would not be in the scope of the project. The volume of calls is dependent mainly on the number of service issues that are raised.

4.3.22. SMS and E-mail Service

a) CSP would be required to provide SMS (Short Message Service) services required to send and receive SMS to end users of the portal as per business requirements of the portal application. SMS to be provided as a service by the Vendor either directly or through a service provider.
b) E-mail services to send e-mails with rich content to end users of the portal as per business requirements would be required to be provided by the service provider.
c) E-mails sent to end users would be required to be stored for reference.
d) E-mails services are required to receive and send e-mails related to support, help etc. from end users of the portal.
e) CSP should provide for e-mail and SMS data archiving and backup.

4.3.23. Proposed Initial Configuration of Private Cloud at DC:

4.3.23.1. Production Environment

The following is the initial minimum requirement of the private cloud for the production/development environment at the primary Data Centre.

Description	vCore	RAM (GB)	Performance Storage (GB)
Production Environment (Compute)			
Web/App Server I	2	4	50
Web/App Server II	2	8	100
Web/App Server III	4	12	50
Web/App Server IV	4	24	100
Database Server (Active)	2	8	100
Database Server (Active)	4	16	100
Database Server (Active)	8	64	100
Services			
Active Directory	Service		
Backup domain controller	Service		
Windows Update	Service		
Application monitoring	Service		
Antivirus Management	Service		
Online Backup	Service		
Software and Licenses			
Windows Server	Service		
MSSQL / Oracle	Service		
Enterprise Management Software for all devices including: ✓ Network monitoring and Management ✓ MSSQL application monitoring ✓ IIS Web service monitoring ✓ Helpdesk management ✓ Change Management ✓ Syslog Management ✓ Private cloud dashboard	Service		
Security Services			
Internal UTM (Throughput up to 1 Gbps)	In No.		
External UTM (Throughput up to 1 Gbps)	In No.		
Network Connectivity			
Unmetered Internet Bandwidth	In No.		
Public IP's	In No.		
Load Balancer (Throughput up to 1 Gbps)	In No.		
Backup Services			
Backup Space	Service		
Backup Agent	Service		
Hosting Services			
One Time Hardware Setup	Service		
OS Management Services	Service		
Backup Management Services	Service		

DB Management Services	Service		
Firewall Management Services	Service		
Anti-virus and anti-malware service	Service		
Malware Trojan scanning service (every day for website)	Service		
VAPT service (Every Quarter)	Service		
DDoS Mitigation Service	Service		
24 x 7 Ticket, Chat & Phone Support	Service		
24 x 7 Monitoring Service	Service		
24 x 7 Website / portal security monitoring / management	Service		

4.3.24. Up-scaling / downscaling of Infrastructure

a) Bidders would not be allowed to downscale the infrastructure below this initial level. However, in order to utilize the benefit of cloud infrastructure, The Purchaser could upscale or downscale infrastructure if the monthly average number of concurrent users are higher or lower than the yearly projected ranges. These would be done through the provisioning portal and reports for resource utilization. Based on the optional rates, being obtained in this RFP, the cost of infrastructure resources being upscale or downscale in such cases, would be added or reduced to / from the quarterly payments on pro-rata basis.
b) All web forms; dashboard and static pages end-to-end response time for the page load including the rendering time shall not be more than 10 seconds. Any page taking more than 10 seconds shall be considered as non-responsive form shall be considered as a defect. This would be checked as part of the quality assurance / testing process.

4.3.25. Severity, Priority and SLAs

a) Service Level requirements will be necessarily managed by the CSP using any tool by the service provider. CSP will make this information available to authorised /Nodal personnel of the Purchaser through on-line browsing and also through hard copy of the report as per requirement. The SLAs primarily would depend on infrastructure issues
b) The success of service level agreements depends fundamentally on the ability to measure performance comprehensively and accurately so that credible and reliable information can be provided to customers and support areas on the service provided.
c) Service factors must be meaningful, measurable and monitored constantly.
d) Service level monitoring will be performed by the Service provider. Reports will be produced as and when required and forwarded to the Purchaser.

Following table describes the severity of the defects:

Table-Severity of Defects

Defect Severity	Business Impact	Resolution Time
S0	Issues causing severe business impact on Data Integrity, Security, UAT, and Transaction Accuracy	60 min - quick-fix 5 working days – permanent resolution
S1	Issues causing high business impact on Functionality, UI/Usability and Response Time	60 min - quick-fix 7 working days – permanent resolution

Defect Severity	Business Impact	Resolution Time
S2	Issues causing moderate business impact on Functionality, UI/Usability, Accessibility which do not block the user to transact	1 day- quick-fix 15 working days – permanent resolution
S3	Issues causing lower business impact on Functionality, UI/ Usability, Compatibility which do not block the user to transact	3 days- quick-fix 15 working days – permanent resolution
Notes: The S0, S1 issues shall be mitigated with 60 minutes of reporting the issue. The S0/S1 issues shall have a permanent resolution deployed on the servers after exhaustive testing within 5/7 working days. For S2/S3 issues permanent resolution shall be deployed within 15 working days.		

Following table describes the Priorities of the defects and resolution SLAs:

Table- Priorities of Defects and Resolution SLAs

Defect Priority	Business Impact	Resolution Details
P0	All Portal users affected. E.g. Portal is not up or Logins are blocked or Application / HH request Submit is not taking place or Payment transactions are processed to incorrect accounts, users are unable to transact in marketplace	Shall be resolved within 45 minutes through a quick-fix engineering. A permanent solution shall be deployed within 2 working days
P1	All users of an application are affected. e.g. applications of a specific Dept. by all users are not being processed, issue in saving offline applications etc.	Shall be resolved within 60 minutes through a quick-fix engineering. A permanent solution shall be deployed within 3 working days
P2	All Dept. Users are affected. E.g. users are not able to view reports or carry out Administrative functions	Shall be resolved within 1 day through a quick-fix engineering. A permanent solution shall be deployed within 4 working days.
P3	A user is affected. E.g. User is not able to enter / process the transaction, specific login issues, mails / alerts / SMS not being sent	Shall be resolved within 1 day through a quick-fix engineering. A permanent solution shall be deployed within 5 working days.

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

Table- Compliance Level for SLAs

Severity or Priority Level	Resolution Time	Penalty
S0 or PO	Resolution Time <= T (As per above tables) from the time the complaint / query is reported for resolution by the helpdesk.	Rs. 5,000 for delay of every additional hour subject to a maximum of 5% of quarterly payment amount.
S1 or P1		Rs. 4,000 for delay of every additional hour subject to a maximum of 5% of quarterly payment amount.
S2 or P2		Rs. 2,500 for delay of every additional hour subject to a maximum of 5% of quarterly payment amount.

S3 or P3		Rs. 1,000 for delay of every additional hour subject to a maximum of 5% of quarterly payment amount.

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	>= 99.95%	Per 0.5% breach of target. This will be calculated monthly after the Go-live of the application. Uptime (%) = $\frac{\text{hours application up in the month}}{\text{total hours in the month}}$ X100	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.			

4.3.26. Change Management

The Purchaser may request, in writing, about the need for a change in the solution. The bidder shall evaluate the change request of The Purchaser, and if the requested change would, in its reasonable opinion, involve additional work or time, the bidder shall convey in writing to The Purchaser the man-days effort required for the Change Request. The effort estimate, corresponding billable amount and planned delivery dates for the change required need to be discussed and mutually agreed in writing.

4.3.27. Project Governance and Management

The Bidder shall provide a detailed Project Plan consisting of (but not limited to) the resource allocation, ownership, responsibilities, risks and mitigation strategies, schedule and milestones, deliverables, sign-off criteria, requirements / inputs from The Purchaser etc.
The Bidder shall communicate to The Purchaser as per mutually agreed periodicity project governance reports for monitoring the project.

4.3.28. IT Assets and Intellectual Properties (IP) Ownership

The Purchaser expects the Bidder to provide hosting of “the Portal/ Website/ application” at their DC along with necessary Hardware, Software, Networking Equipment and Solutions and Manage the DC Operation.

The Bidder may propose to implement in-house / third-party software solutions or develop custom solutions or combination of the both to meet "the Portal/ Website/ application" requirements specified in this document.
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. No.	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							

4.3.29. Responsibility Matrix

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

Table- Responsibility Matrix

Sl No.	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 & DR	**Y**		
9.	Provisioning of the required hardware for IaaS Cloud	**Y**		
10.	Network Connectivity between IaaS Cloud and the DR site	**Y**		

11.	Internet Connectivity provisioning IaaS Cloud and the DR site	**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 (Cloud to DR)	**Y**		
17.	Switch Over Testing (DR to Cloud)	**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. Pre-qualification eligibility Criteria

1. MeitY empanelled Cloud Service Providers (CSP) or their authorized Managed Service Providers (MSP) can bid in response to this RFP, provided the compliance requirements are met.
2. The MSP can either be the CSP itself or an MSP (an authorized partner of the CSP). In case of CSP is bidding directly, it cannot authorize its partners to submit another bid for CSP's solution. It is the responsibility of the selected MSP to ensure and meet the entire Scope of Work mentioned in this RFP.
3. An MSP can submit only one bid with the authorization of any one CSP and cannot propose solutions of multiple CSPs in its bid.
4. In case an MSP wins the Tender, a tripartite Agreement shall have to be executed between the OCAC, the Successful Bidder (MSP) and the corresponding CSP.
5. The CSP should have obtained valid Audit Certificate either directly from STQC or from an agency empanelled with CERT-IN.

5.1. Pre-qualification

Sl. No.	Clause	Documents Required
1.	The bids should be submitted by only Prime Bidder, no consortium is allowed in this bid.	Declaration in this regard needs to be submitted.
2.	The Bidder should have positive net worth during last three financial years, ending 31.03.2021.	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) 5 cores in last three financial years and profitable during each of the previous three financial years ending on 31.03.2021. Note: The turnover refers to the Bidder's firm and not the composite turnover of its subsidiaries/sister concerns etc.	Copy of audited profit and loss account/ balance sheet/ annual report of the last three financial years.
4.	The bidder must be registered under the Companies Act 1956 or a Partnership firm registered under LLP Act, 2008 and must have in operation for a period of at least 5 (Five) years as of March 31, 2021. The company must be registered with appropriate authorities for all applicable statutory duties/taxes	(a) Valid documentary proof for :- ✓ Certificate of incorporation (b) Valid documentary proof for: ✓ GST Identification number (GSTIN) ✓ Income Tax registration/PAN number ✓ Up to date GST Return ✓ Income Tax returns for last three financial years.
5.	The CSP in India must have average turnover of at least 2000 Crore for last 3 financial years and must have positive net worth in each of the last three financial years.	Copy of audited balance sheet/annual report of the last three financial years. Chartered Accountant certificate for net worth and turnover
6.	CSP authorization	In case the bidder isn't a CSP, the bidder has to submit authorization certificate from CSP to participate and quote against this RFP.

Sl. No.	Clause	Documents Required
7.	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
8.	The Bidder must have a registered Branch office in Odisha or if not having office in Odisha should submit an undertaking to open office within one month after getting the Purchase Order. The Bidder must have 10 IT Service Engineer/ Professionals out of which 5 professionals should be certified on the quoted CSP product.	Office Address or Undertaking A self-certified letter by an authorized signatory mentioning the list of IT service engineer/ professionals. CSP certification of certified professionals.
9.	The CSP data centre hosting facility should be empanelled under MeitY and tier III or higher certified.	Copy of valid compliance certificate for Tier-III or higher as per TIA 942 or Uptime Certification
10.	Quality Certification of bidder	Valid ISO 9001, ISO 27001, ISO 20000, CMMi level 3 or higher of the bidder
11.	Bid security declaration	Bid Security Declaration to be submitted
12.	RFP document fee of Rs. 11,200/- (inclusive of 12% GST)	

6. Technical capabilities of CSP

Sl. No.	Description	Compliance (Yes/ NO)	Deviations if any
1	CSP should be operating in India for at least 5 years as a cloud service provider.		
2	CSP should be a registered firm or a company in India and the proposed Data Centres (DC & DR) should have jurisdiction in India		
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.		
5	CSP to have ISO-22301 certification for business continuity.		
6	CSP should be present in latest Gartner Magic Quadrant for “Cloud Infrastructure and platform as a Service”.		
7	The CSP should provide all variants of cloud service as per MeitY guidelines. o Infrastructure as a Service (IaaS), o Platform as a Service (PaaS) o Software as a Service (SaaS)		
8	The CSP must ensure against any breach of data security and data loss of hosted applications.		
9	CSP should support both BYOL (Bring your own license) as well as PAYG (Pay as you go). The OS offered should come with continuous updates and upgrades for the entire contract duration.		
10	CSP should have accreditations relevant to security, availability, confidentiality, processing integrity, and/or privacy Trust Services principles. SOC 1, SOC 2, SOC 3.		
11	Data Centres should be compliant at a minimum with the following: o ISO 9001 o ISO/IEC 20000 o ISO/IEC 27001 o ISO/IEC 27017 o ISO/IEC 27018 o ISO/IEC 27701 o PCI DSS Level 1		
12	CSP should support a minimum uptime of 99.99% for each of its services. A publicly available documentation needs to be provided for the same.		
13	The CSP must support dedicated connectivity from at least 3 ISP providers for department/organization to choose between at the time of deployment.		

7. Instruction to Bidders

- 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.
- 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.
- Bidder has to select the payment option as per the tender document to pay the tender fee / Tender Processing fee.
- 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.
- Technically qualified bidders will be considered as successful bidders for price bid opening.
- The bidder must submit all documents as asked in Annexure section.

7.1. Bid Security

Bid Security Declaration to be submitted by the Bidder as per the prescribed format attached in this RFP.

7.2. Completeness of the RFP Document

a) 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.
b) 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:
    - Include all documentation specified in this RFP document;
    - Follow the format prescribed in this RFP document and respond to each element in the order as set out in this RFP document.
    - Comply with all requirements as set out within this RFP document.

7.3. Pre-Bid Meeting and Amendment to the Tender Document

a) Pre-Bid Meeting of shortlisted bidders is scheduled as per the details specified in the RFP. The objective of this meeting is to address the queries of the bidders related to the Project.
b) Bidders may request a clarification/suggestion of any Item/ Clause of the RFP document on or before 20/07/2022 at 05:00 PM. Any request for clarification must be sent in electronic mail to the below address: sk.bhol@nic.in and osdc@ocac.in.

All enquiries / clarifications/ suggestion from the shortlisted bidders, related to this RFP, must be directed in writing exclusively to the contact person notified in this RFP document.
c) The preferred mode of delivering written questions to the aforementioned contact person would be through e-mail. Telephone calls will not be accepted. In no event will the OCAC

be responsible for ensuring that bidder's inquiries have been received by OCAC. The queries by the bidders will be provided in the following format. Request for clarifications Format:

Company Name	**Person Name**	**Designation, E-Mail, Contact Number**	
Page No	**Clause**	**Sub-Clause**	**Suggestion**

d) At any time till 10 days before the deadline for submission of bids OCAC Bhubaneswar may, for any reason, whether an own initiative or in response to a clarification requested by shortlisted Bidder, modify the bidding document by amendment.
e) All amendments made in the document would be published in the website www.ocac.in, www.odisha.gov.in and www.gem.gov.in.
f) Shortlisted Bidders are also advised to visit the aforementioned website on a regular basis for updates. OCAC Bhubaneswar also reserves the right to amend the dates mentioned in cover page for the bid process.

7.4. Evaluation Criteria

a) 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.
b) 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.
c) The Evaluation Committee may ask for technical presentation from the Shortlisted Bidders in reference to the scope of work mentioned in this RFP.
d) The Commercial Bids of the qualified bidders will be evaluated based on the submitted artifacts/ annexure.
e) After opening of financial bid, lowest financial quote will be considered as L1.

8. General Terms & Conditions of Tender

8.1. General

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

- **Health and Safety**: The Bidder and any of its valid MSP shall, when at OCAC site, conduct their activities so that their equipment, working conditions and methods are safe and without risk to health for their own and OCAC's employees as well as for any other users of OCAC Site.
- **No Joint Venture:** Nothing contained in this RFP shall be construed as creating a joint venture, partnership or employment relationship between the parties, nor shall either party have the right, power or authority to create any obligation or duty, express or implied, on behalf of the other.
- **No Assignment:** Except with respect to The Bidder's rights regarding the use of MSP, neither party may assign any rights or obligations under this Contract without the prior written consent of the other party except to the surviving entity in a merger or consolidation in which it participates or to a purchaser of all or substantially all of its assets, so long as such surviving entity or purchaser shall expressly assume in writing the performance of all of the terms of this Agreement.

The Bidder shall ensure that the software and allied components used to service OCAC are licensed and legal.

8.2. Performance Bank Guarantee (PBG)

The Bidder shall furnish a **Performance Bank Guarantee (PBG) for 3% (three 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.

8.3. Award Criteria

Lowest financial quote will be considered as L1.

8.4. 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.

8.5. Submission of Bid

Bid to be submitted online at GEM Portal Only.

8.6. Deadline for Submission of Bids

The deadline for submission for this RFP is as per scheduled defined, unless any corrigendum published for extension.

8.7. Project Time Line & Terms of Payment

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

SL. NO.	Description	Time Line	Payment Terms
1.	Provisioning of a) Data Centre & DR b) IT Infrastructure installation in Racks of DC&DR c) Network Connectivity	Within 1 week from the issuance of LOI	Nil
2.	Migration of the application on the new Cloud environment (if any)	Within 1 week 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 Payment as per utilisation of resource

a) The successful Bidder has to sign an agreement on non-judicial stamp paper.
b) In case the Bidder fails to execute the contract, The Purchaser shall have liberty to get it done through any other vendors with full cost recoverable from the Bidder in addition to damages and penalty.
c) All payments shall be subject to current applicable statutory taxes.
d) The rate quoted should be firm.
e) In case of any difference between the rates quoted in figures and words, the latter shall prevail.

8.8. Termination of Contract

❖ **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:

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

❖ **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 **three years** 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 a the contracted rates.

8.9. 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.

8.10. 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.

8.11. 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.

8.12. 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.

8.13. 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.

8.14. 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.

8.15. 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:

- "Corrupt practice" means the offering, giving, receiving or soliciting of anything of value to influence the action of the Purchaser in contract executions.
- "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.
- "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
- "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.
- "Coercive Practices" means harming or threatening to harm, directly or indirectly, persons or their property to influence their participation in the execution of contract.

- 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.

8.16. Exit Management

(A) 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.

(B) 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:

- 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;
- 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.
- 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).
- 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.
- Bidder will sign a Non-Disclosure Agreement with The Purchaser. The format for the same has been included in Annexure.

(C) 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.

(D) 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.

(E) 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.

8.17. 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.

8.18. Billing

The Bidder shall specify the Branch/ Location from which they will raise the bill and in whose favour payment will be released.

8.19. 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, provided that any printed literature furnished by the Bidder may be written in another language so long as it is accompanied by an English translation in which case, for purposes of interpretation of the Bid, the English translation shall govern.

8.20. 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.

8.21. 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.

8.22. 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.

8.23. 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.

8.24. 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.

8.25. Confidentiality

- 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.

- The Bidder shall not without the Purchaser prior written consent, make use of any document or information.
- 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.

8.26. 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.

8.27. 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.

The Bidder shall specify the Branch/ Location from which they will raise the bill and in whose favour payment will be released.

8.28. Limitation of Liability towards the Purchaser

a) 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.
b) 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.
c) 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.

d) 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.

8.29. Changes of Orders

a) The Purchaser may at any time, by written order given to the Bidder, make changes within the general scope of the Contract.

b) 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 adjustments 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.

c) 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.

8.30. Term and Extension of the Period

a) The term under this Contract will be for a period of 36 months which shall start from day of signing of the Contract.

b) 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.

c) 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.

d) 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.

8.31. 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.

8.32. Resolution of Disputes between the Purchaser and engaged Bidder

a) 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.

b) 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.

c) 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.

d) 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.

8.33. 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.

9. Annexure(s) - Bid Formats

9.1. 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.)
		2018-19	
		2019-20	
		2020-21	

Signature of the Bidder
Date:
Place:

Company Seal

9.2. 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

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:

Signature of the Bidder
Date:
Place:

Company Seal

9.3. 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:

Signature of the Bidder
Date:
Place:

Company Seal

9.4. Annexure (T4): 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

In response to the RFP No._____, Ms./ Mr. _____, as a _____, I / We hereby declare that our company _____is having unblemished past record and have not been declared blacklisted by any Central/State Government/PSU institution and there has been no pending litigation with any government department on account of similar services.

I/We further declare that our company has not defaulted in executing any Government order in the past.

Signature of witness
Date:
Place:

Signature of the Bidder
Date:
Place:

Company Seal

9.5. 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

9.6. Annexure (T6): Technical Compliance for cloud requirements

Bidder must fill up the following compliance table for cloud requirements. Compliance against these heads would imply compliance against all parameters / activities mentioned under respective heads below. These requirements are mandatory and in case of non-compliance, the Bidder may not be qualified for commercial evaluation at the discretion of OCAC.

#	**Section in RFP**	**Description**	**Compliance (Yes / No)**
1.	5.2	General Requirements	
2.	5.3.1	General Cloud Requirements	
3.	5.3.2	DR Management and BCP	
4.	5.3.4	Cloud Service Provisioning requirements	
5.	5.3.5	Data Management	
6.	5.3.6	Operational Management	
7.	5.3.7	Compatibility Requirements	
8.	5.3.8	Cloud NW Requirements	
9.	5.3.9	Cloud Storage Service Requirements	
10.	5.3.10	Portal Security	
11.	5.3.11	Non-Compliance of Portal Security Audit	
12.	5.3.12	Cloud Security Requirements	
13.	5.3.13	Virtual Machine Requirements	
14.	5.3.14	Cloud Resource and NW Monitoring	
15.	5.3.15	Application Performance Monitoring	
16.	5.3.16	Backup Services	
17.	5.3.17	WAF as Service	
18.	5.3.18	MMS, AA, EXT. VAS	
19.	5.3.19	DSS	
20.	5.3.20	Managed Services	
21.	5.3.21	Helpdesk support	
22.	5.3.23	Configuration of Private Cloud	
23.	5.3.24	Up-scaling /down-scaling of Infra	
24.	5.3.25	SLAs	
25.	5.3.26	Change Management	
26.	5.3.27	PG&M	
27.	5.3.28	IT Assets and IP ownership	
28.	5.3.29	RM	

Signature of the Bidder

Place & Date

Company Seal

9.7. 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			
2			

Signature of the Bidder

Place & Date

Company Seal

9.8. Annexure (T8): Compliance Check List

RFP No: _____, Date: _____

Please check whether following have been enclosed.

Sl. No	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 (Annex-T1)		
4.	Self-Declaration that the bidder hasn't been black listed / performance issues by any Govt./PSU (Annex-T2, T4)		
5.	Acceptance of Terms & Conditions Contained In The Tender Document (Annex-T3)		
6.	Representative Authorization Letter (Annex-T5)		
7.	Annexure T6-Technical Compliance		
8.	Annexure T7- Statement of Deviations		
9.	Bid Security Declaration, RFP Document Fee		

Signature of the Bidder

Place & Date

Company Seal

9.9. Annexure (T9): Bid Security Declaration

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

To
General Manager (Admin.)
Odisha Computer Application Centre
OCAC Building, Plot No. N-1/7-D
Acharya Vihar Square, RRL Post Office
Bhubaneswar - 751013

Reference: (1) Enquiry No. _____.

(2) Our Bid No. _____ date _____.

I/ We, _____ irrevocably declare as under:

I/ We understand that, as per Clause _____of Tender/ bid conditions, bids must be supported by a Bid Security Declaration in lieu of Earnest Money Deposit.

I/ We hereby accept that I/ We may be disqualified from bidding for any contract with you for a period of **Three Years** from the date of disqualification as may be notified by you (without prejudice to OCAC's rights to claim damages or any other legal recourse) if,

1) I am /We are in a breach of any of the obligations under the bid conditions,
2) I /We have withdrawn or unilaterally modified/ amended/ revised, my/our Bid during the bid validity period specified in the form of Bid or extended period, if any.
3) On acceptance of our bid by OCAC, I /we failed to deposit the prescribed Performance Bank Guarantee (PBG) or fails to execute the agreement or fails to commence the execution of the work in accordance with the terms and conditions and within the specified time.

Signature:

Name & designation of the authorized person signing the Bid-Securing Declaration Form:

Duly authorized to sign the bid for and on behalf of: _____ (complete name of Bidder)

Dated on _____ day of _____ month, _____ year.

9.10. 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:

9.11. Annexure (P2): Price Bid

These below rates may also be used for any cloud service requirements for any ICT projects for the Purchaser /Departments/Agencies/Directorates and should be valid for the project duration of three years. These prices would also be used for up-scaling and downscaling of infrastructure as mentioned in RFP.

COMPUTE SERVICES			
Sl. No.	**Description**	**Price per month for windows server inclusive of Tax**	**Price per month for Linux server inclusive of Tax**
1	VM Server Instance Type 1(vCPU-2, RAM-4 GB, Storage-50 GB)		
2	VM Server Instance Type 2(vCPU-2, RAM-8 GB, Storage-100 GB		
3	VM Server Instance Type 3(vCPU-4, RAM-12 GB, Storage-50 GB)		
4	VM Server Instance Type 4(vCPU-4, RAM-24 GB, Storage-100 GB)		
5	VM Server Instance Type 5(vCPU-6, RAM-12 GB, Storage-100 GB)		
6	VM Server Instance Type 6(vCPU-6, RAM-24 GB, Storage-200 GB)		
7	VM Server Instance Type 7(vCPU-8, RAM-24 GB, Storage-200 GB)		
8	VM Server Instance Type 8(vCPU-8, RAM-48 GB, Storage-200 GB)		
9	VM Server Instance Type 10(vCPU-16, RAM-64 GB, Storage-200 GB)		
10	VM Server Instance Type 11(vCPU-16, RAM-128 GB, Storage-400 GB)		

STORAGE SERVICES			
Sl. No.	**Description**	**Quantity**	**Price per month inclusive of Tax**
1	Block storage(100 GB)	1	
2	Block Storage(1 TB)	1	
3	Object Storage (100 GB)	1	
4	Object Storage (1 TB)	1	
5	File Storage (100 GB)	1	
6	File Storage (1 TB)	1	
7	Archive Storage (1 TB)	1	

DATABASE SERVICES			
Sl. No.	**Description**	**Sizing (Core, RAM)**	**Price per month inclusive of Tax**
1	Managed (PostgreSQL / MySQL/ Maria/ Mango DB) with 100 GB storage	2, 8	
2	Managed (PostgreSQL / MySQL/ Maria/ Mango DB) with 100 GB storage	4, 16	
3	Managed (PostgreSQL / MySQL/ Maria/ Mango DB) with 100 GB storage	8, 64	
4	MS SQL Enterprise Edition Latest with 100 GB storage	2, 8	
5	MS SQL Enterprise Edition Latest with 100 GB storage	4, 16	
6	MS SQL Enterprise Edition Latest with 100 GB storage	8, 64	

7	Oracle Enterprise Edition Latest with 100 GB storage	2, 8	
8	Oracle Enterprise Edition Latest with 100 GB storage	4, 16	
9	Oracle Enterprise Edition Latest with 100 GB storage	8, 64	
10	Additional 100 GB for managed database	1	
11	Additional 100 GB for MS SQL enterprise	1	
12	Additional 100 GB for Oracle database	1	
NETWORK SERVICES			
Sl. No.	**Description**	**Quantity**	**Unit of Price per month inclusive of Tax**
1	Load Balancer with SSL Offloading	1	
2	Static Public IP with NAT	1	
3	DNS Manager per DNS	1	
4	Remote VPN connectivity (IPSec VPN/SSL VPN)	10	
5	Dedicated connectivity between OCAC & cloud DC (100 Mbps)	1	
SECURITY SERVICES			
Sl. No.	**Description**	**Quantity**	**Unit of Price per month inclusive of Tax**
1	Managed Virtual Firewall and IPS	1	
2	Enterprise Anti-virus and Anti Malware Protection	1	
3	Managed Web Application Firewall	1	
4	DDoS Protection Service	1	
5	Vulnerability analysis and penetration testing	Per time	
BACKUP & DR SERVICES			
Sl. No.	**Description**	**Quantity**	**Unit of Price per month inclusive of Tax**
1	VM backup per VM up to 500 GB disk	1	
2	Disk backup per TB	1	
3	Disk snapshot per TB	1	
4	1 TB data transfer from OCAC to cloud DC	1	
CLOUD MANAGEMENT AND MONITORING SERVICES			
Sl. No.	**Description**	**Quantity**	**Unit of Price per month inclusive of Tax**
1	Cloud management & monitoring tool dashboard – Application, Database Performance, Hardware, Network Monitoring, Asset MGT Configuration, SMS Subscription Service(In bulk of 300) and Audit Trail	1	
ADDITIONAL RESOURCES			
Sl. No.	**Description**	**Quantity**	**Unit of Price per month inclusive of Tax**
1	2 Virtual CPU	1	

2	4 GB RAM	1	
3	50 GB Block Storage	1	
4	50 GB File Storage	1	
5	50 GB Object Storage	1	
6	2 MBPS Internet Link	1	
GRAND TOTAL			

Rupees (in words):

_____

Signature & seal of the Bidder

Place & Date:

9.12. 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***