Department of Agriculture and Farmer's Welfare Bid Document

Selection of Managed Service Provider for providing Cloud Services to the Department of Agriculture and Farmer's Welfare

FACTSHEET

Sr. No.	Item No.	Details
A.	Bid/Tender No.	As per GeM
B.	Name of the Work/Project	RFP for Cloud Service Provider for providing Cloud Hosting and Managed Services for the Department of Agriculture and Farmers' Welfare
C.	Name of the issuer of this Tender	Director (Farmers Welfare, Digital Agriculture), Department of Agriculture and Farmers' Welfare, Ministry of Agriculture and Farmers' Welfare, Government of India
D.	Date of issue of Tender Document	As per GeM
E.	Date of Pre-Bid meeting	As per GeM
F.	Last Date for submission of Bid	As per GeM
G.	Date of Bid Opening	As per GeM
H.	Mode of Bid Opening	As per GeM
I.	Bid Language	Bid should be submitted in English language Only
J.	Bid Submission documents checklist	As per GeM
K.	Period of Engagement	As per GeM / 3 years
L.	Address of Communication	Under Secretary (Digital Agriculture), Department of Agriculture and Farmers' Welfare, Ministry of Agriculture and Farmers' Welfare, Government of India Email : us-it@gov.in Phone : 011-23382926
M.	Earnest Money Deposit (EMD)	As per GeM
N.	Processing Fee (Non-Refundable)	As per GeM
O.	Availability of Tender Document	As per GeM
P.	Validity of Proposal	Proposals must remain valid for 180 days after the submission date.
Q.	General Terms and condition	As per RFP
R.	Consortium	Not allowed
S.	Method of Selection	Quality cum Cost Based Selection
T.	Bid Submission	As per GeM
U.	Performance Bank Guarantee	As per GeM

DISCLAIMER

The information contained in this RFP Document or subsequently provided to Bidder(s) or Applicants whether verbally or in documentary form by or on behalf of this RFP, or any of their employees or advisors, is provided to the Bidder(s) on the terms and conditions set out in this RFP Document and all other terms and conditions subject to which such information is provided.

This RFP document is not an agreement and is not an offer or invitation to any party other than the Applicants who are qualified to submit the Bids (“Bidders”). The principle (purpose) of this RFP Document is to provide the Bidder(s) with information to support the formulation of their Proposals. This RFP Document does not purport (claim) to contain all the information each Bidder may entail (require). This RFP Document may not be appropriate for all persons, and it is not possible for the team managing RFP or advisors to consider the investment objectives, financial situation, and particular needs of each Bidder who reads or uses this RFP Document. Each Bidder should conduct its own investigations and analysis and should check the accuracy, reliability, and completeness of the information in this RFP Document and where necessary obtain independent advice from appropriate sources. The Department of Agriculture and Farmers’ Welfare (DA&FW), and their employees and advisors make no representation or warranty and shall incur no liability under any law, statute, rules or regulations as to the precision (accuracy), reliability or completeness of the RFP Document. DA&FW may in their absolute discretion, but without being under any obligation to do so, update, improve or supplement the information in this RFP Document.

The issue of the RFP does not imply that the DA&FW is bound to select any Bidder or to appoint the Cloud Service Provider, as the case may be, for the Project, and the DA&FW reserves the right to reject all or any of the proposals without assigning any reasons whatsoever. The Bidder shall bear all its costs associated with or relating to the preparation and submission of its Proposal including but not limited to preparation, copying, postage, delivery fees, and expenses associated with any demonstrations or presentations which may be required by the DA&FW or any other costs incurred in connection with or relating to its Proposal. All such costs and expenses will remain with the Bidder and the DA&FW shall not be liable in any manner whatsoever for the same or for any other costs or other expenses incurred by an applicant in preparation or submission of the Proposal, regardless of the conduct or outcome of the selection process.

DA&FW also reserves the right to withdraw this RFP without assigning any reason and without any liability to the Bidder or any other person or party.

Glossary of Terms

Acronym	Expansion
MSP	Managed Service Provider
EMD	Earnest Money Deposit
EMI	Equated Monthly Installment
EQI	Equated Quarterly Installment
GI Cloud	Government of India Cloud
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
IOPS	Input/output operations per second
MSP	Managed Service Provider
O&M	Operations and Maintenance
NRC	National Register of Citizens
PaaS	Platform as a Service
PBG	Performance Bank Guarantee
PCI DSS	Payment Card Industry Data Security Standard
RPO	Recovery Point Objective
RTO	Recovery Time objective
SAS	Serial Attached SCSI
SATA	Serial Advanced Technology Attachment
SCSI	Small Computer System Interface
SI	System Integrator
SLA	Service Level Agreement
SSD	Solid State Drive
VLAN	Virtual Local Area Network
VLB	Virtual Load Balancer
VM	Virtual Machines

Contents

1. Introduction:

1.1. About Department of Agriculture and Farmers' Welfare (DA&FW):

The Department of Agriculture and Farmers' Welfare (DA&FW) is one of the two constituent Departments of the Ministry of Agriculture and Farmers' Welfare, and the Department of Agricultural Research and Education (DARE). The Department of Agriculture and Farmers Welfare is headed by Agriculture and Farmers Welfare Minister and is assisted by two Ministers of State. The Secretary (DA&FW) is the administrative head of the Department. The Secretary is assisted by two Additional Secretaries including one Financial Adviser, 12 Joint Secretaries including Mission Director (Mission on Integrated Development of Horticulture) and Mission Director (National Mission on Sustainable Agriculture), Horticulture Commissioner, Trade Advisor, Horticulture Statistics Advisor, Addl. Deputy Director General and Deputy Director General. In addition, the Chairman the of Commission for Agriculture Costs and Prices (CACP) advises Department on pricing policies for selected agricultural crops.

The DA&FW is organized into 28 divisions and has five attached offices and twenty-one subordinate offices which are spread across the country for coordination with state-level agencies and implementation of Central Sector Schemes in their respective fields. Further, one Public Sector Undertaking, seven autonomous bodies, and two authorities are functioning under the administrative control of the Department.

2. Purpose of the Bid

Department intends to issue this tender document, to eligible entities, to participate in the competitive bidding for appointment of a vendor for providing Cloud Hosting and Managed Services for the use of department, its sub-ordinate officers as well as autonomous organizations under the department. Most Schemes such as PM-KISAN, Agri stack Project PMFBY, E-NAM, Soil Health, Farm Machinery, Crops, Seeds, Horticulture, Plant Protection etc. under the Department of Agriculture and Farmers' Welfare are currentlyhosted on the cloud. Also, if any new requirement arises that will also be hosted on the cloud infrastructure.

For this purpose, the Department of Agriculture and Farmers Welfare, Gov of India (herein after called DA&FW), invites proposals for primarily Cloud hosting and other activities mentioned under the Project Scope in respect of procuring Cloud Services and Managed Services for the schemes under the Department of Agriculture and Farmers' Welfare, sub-ordinate offices as well as autonomous organizations.

The Proposed Services should be managed with SLA driven, scalable, extensible, highly configurable, secure, and very responsive way.

2.1. Requirement of Cloud Services

Considering the growing adoption of online services and the use of IT within the Government, there is a constantly increasing demand from Departments for infrastructure for hosting services including disaster recovery and backup for their various IT applications.
Department requires the cloud service provider to extend its IT requirements as per demand. The cloud service provider should follow the below basic compliance requirement:

- MeitY has empaneled the Cloud Service offerings of MSPs in the form of Bouquet of Cloud Services.
- The cloud service provider should be listed on the GeM portal.
- CSP should be MeitY empaneled. The proposed Data Centre for hosting should be clearly mentioned and same must be mentioned on the https://meity.gov.in.
- CSP shall offer DR cloud services with their Data Centre location within India only. All the physical servers, storage, and other IT hardware from where cloud resources are provisioned for department must be within Indian Data Centre only. CSP shall ensure that department data resides within India only.
- All monitoring, provisioning, should be within India and 100% isolated from other regions outside India, if in case MSP has Global presence.
- The MSPs shall comply or meet any security requirements applicable to Bidder published by the Government bodies such as CERT-IN, NCIIPC etc. at the time of bid submission. The Bidder shall meet all the security requirements indicated in the IT Act 2000, the terms and conditions of the Provisional Empanelment of the Bidders.
- The pricing should be considered after providing 60 days of free trail services from the date of award of contract or date of deployment of cloud resource / service.
- The bidder is expected to provide setup and services with a zero capital (one-time) cost.
- All the components mentioned will follow Pay as you go pricing model on actual consumption.
- The department is not bound to avail all the services mentioned in the list.
- The quantity and configuration of the service requested may vary in future, and the bidder needs to make the provision for accommodating the same.
- This Cloud will be used for various projects under the Department of Agriculture and Farmers' Welfare (DA&FW) and its attached offices, societies, autonomous institutions and other entities under DA&FW.

3. Scope of Work:

The broad project scope includes having a single service provider to managed services for cloud infrastructure. The department intends to procure the 'Cloud Hosting and Managed Services' for the business applications. The shortlisted service provider shall provide the Cloud Hosting and Complete Managed Services through this bidding process for the period of 3 years, department reserves the right to extend the services for another 2 years.

The proposed solution shall be scalable, extensible, highly configurable, secure, and very responsive and shall support integration and optimization including scale up and scale down of required services and solutions (existing legacy and acquired in future), designed for or used by the department or department may undergo in up-gradation.

The broader requirements are expressed below –

- Cloud Infrastructure for Application Hosting (DC and DR).
- End to End Managed Service
- Application Migration from existing cloud(if needed)
- Optional Rate Card

Note:

- DR should be able to execute all the business operations smoothly in case of any disaster at primary site (DC).
- MSP has to factor all security components as per the MeitY guidelines and relevant Indian IT acts.

3.1. Managed Services

The department is looking forward for the delivery of the following broad areas of services under this project:

3.1.1 *Design of cloud infrastructure*

- MSP shall set up and manage the entire cloud solution deployed for department by

Provisioning and Managing Cloud based resources on subscription based / OPEX Model only. The MSP should specify the DC and DR site location. department may, at any point of time, undertake audit of the provisioned cloud environment; MSP is required to facilitate such timely audits as decided by the department.

- The Disaster Recovery site shall be on Active - passive within the RPO and RTO defined in the RFP
- The proposed requirement is of DC and DR will be 100% of DC and can be changed later by the Department
- The Managed Service Provider (MSP) is required to have a Near Disaster Recovery (NrDR) site/Multi-AZs architecture within the same metropolitan area as the Primary Data Center (DC), ensuring an active-active configuration for both compute and storage resources.
- MSP shall adequately size the necessary compute, memory, and storage required, building the redundancy into the architecture (including storage) and load balancing to meet the service levels (cloud services) mentioned in the RFP and the application service levels. MSP shall provide a detailed solution document for setting up of the DC and DR. The same shall be approved by the department project in-charge.
- Subsequently, the MSP shall provision the entire infrastructure (compute, storage, network, security, software, bandwidth etc.) required for setting up of the DC and DR site as per the approved solution document.
- MSP shall provide monthly capacity planning reports with recommendations so that informed decision can be taken. MSP shall carry out the capacity planning, accordingly, and on additional capacity to meet the user growth and / or the peak load requirements to support the scalability and performance requirements of the solution. There should not be any constraints on the services.
- The MSP shall ensure that all peripherals, accessories, sub-components required for the functionality and completeness of the solution, including but not limited to devices, equipment, accessories, software, licenses, tools, etc. should also be provisioned according to the requirements of the solution.
- The department will not be responsible if the MSP has not provisioned some components, subcomponents, assemblies, and sub-assemblies as part of bill of material in the bid. The MSP will have to provision the same to meet the solution requirements at no additional cost and time implications to department.
- The Cloud services billing shall be done monthlyon the fixed discount % discovered through the RFP bid process based on per SKUs or Category - Whichever offers higher discount %

3.1.2 *Infrastructure Analysis and Build*

- MSP shall provide complete hardware details at DC and DR site including following parameters
  - CPU Calculation
  - RAM Calculation
  - Disk Calculation
  - Network interface requirement
  - Network throughput requirement
  - Backup requirement
- MSP shall provide direct leased-line connections between the location decided by the department and DC site and department and – DR site, if required or secured access has to be provided to office users.
- Proposed solution should be compatible with IPv6 and High-level architectural diagram showing different layers of solution like Internet / P2P Connectivity, Network, Security,

Compute, Hardware, Storage and Backup layers.

- Proposed solution should have IP schema depicted at high level with NATing to secure the applications directly getting exposed to Internet. MSP should propose to deploy different applications, Web Server, App Servers and database in different VLANs with restricting users to directly access database layer and storage layer.

- MSP shall provide Backup solution with different features, like snapshots of VMs, RDBMS backup, incremental and full back up of all data, restoration of data in test environment or on premises as and when required.

3.1.3 *Scaling of Resources*

- The initial sizing and provisioning of the underlying infrastructure (including the system software and bandwidth) shall be carried out based on the information provided in the RFP.

- Subsequently, the MSP shall scale up (or scale down) the resource requirements (compute, memory, storage, bandwidth etc.) based on the growth in the user compute load / data load / bandwidth load (during peak and non-peak periods / year- on-year increase) to support the scalability and performance requirements of the solution and meet the SLAs. There should not be any constraints on the services.

- Up to 50% scaling up / scaling down should happen automatically. if beyond 50 % then MSP shall provide the necessary details including the sizing calculations, assumptions, current workloads and utilizations, expected growth / demand and any other details justifying the request to scale up or scale down and take prior approval by the department. MSP shall provision the sufficient additional VMs to meet the requirement.

- For any changes to the underlying cloud resources provisioned under the scope of this RFP, department shall get alerts / notifications from the MSP, both as advance alerts and post implementation alerts.

3.1.4. *Ownership of Data / VMs/ Software*

- Department shall retain ownership of all data and applications etc. hosted on infrastructure of MSP and CSP. Department maintains the right to request/retrieve full copies of these at any time (without additional charges).

- Department retains ownership of loaded software installed on virtual machines and any application or product that is deployed by department on the Cloud Infrastructure.

3.1.5 *Compliances*

- MSP shall adhere to the standards published (or to be published) by MeitY for procurement of Cloud Services/ department or any standards body setup / recognized by Government of India and notified to the MSP by department as a mandatory standard.

- The cloud service offerings of MSP/CSP shall always remain Empaneled / complied with the MEITY guidelines and standards. MSP shall be responsible for the costs associated with implementing, assessing, documenting, and maintaining such Empanelment/Compliances.

- MSP shall always remain adhered to the prevailing guidelines issued by NCIIPC, RBI, CERT-In, MoP etc. from time to time.

3.1.6 *Documentation*

- MSP shall create and maintain all the necessary technical documentation, design documents, standard operating procedures, configurations required to continued operations and maintenance of cloud services.

- All the documents, process, policies shall have to be approved by department before release.

- The MSP shall develop, maintain, update following documents as per department requirements:
    - Details of inventory for Compute, Storage, Network, Security elements.
    - Details of the management, monitoring, and helpdesk tools
    - The WAN connectivity plan
    - Business Continuity/DR plan
    - Details of manpower deployment at NOC and SOC
    - Escalation matrix.
    - Other details as desired by department

3.2. General Requirements

3.2.1 *Resource Management*

- The MSP shall provision for Bring your own License (BYOL) by the department if any
- The MSP shall enable workflow based automatic switch over/ failover between DC and DR.
- The MSP shall provision two step authentication of security uniform for all for the following:
    - Service Level Agreements (SLAs)
    - Help Desk and Technical Support
    - Resources (Documentation, Articles/Tutorials, etc.)

3.2.2 *Operation Services*

- MSP shall ensure the overall reliability and responsive operation of the underlying cloud services through both proactive planning and rapid situational response.
- MSP/CSP shall manage the network, storage, server, and virtualization layers, to include performance of internal technology refresh cycles applicable to meet the SLAs.
- MSP shall ensure monitoring of performance, resource utilization and other events such as failure of service, degraded service, availability of the network, storage, database systems, operating Systems, applications, including API access within the MSP's boundary.
- The MSP shall facilitate Cloud console access to the Department to monitor the overall Cloud resource consumption.
- The MSP shall also facilitate admin access to the said cloud console on request.
- The MSP shall facilitate dashboards to monitor Cloud resource utilization to all application owners and TSU team .
- MSP shall coordinate with the respective application owner to ensure the Cloud resource utilization is not below 50%.
- Prepare a comprehensive O&M plan for managing the cloud services and keep it updated.
- MSP shall ensure uptime and utilization of the cloud resources as per SLAs defined in this RFP.
- MSP shall manage the cloud infrastructure as per standard ITIL framework.
- Infrastructure provisioned and managed by MSP should be highly available, scalable, resilient and fault tolerant. Update to all latest patching, upgrade, security vulnerability should be taken care of by MSP in such a manner that it should not bring any outage of application. If there are outages, MSP should submit Root Cause Analysis and promptly take corrective action.
- MSP shall design and implement automated scaling processes.
- Any required version/Software /Hardware upgrades, patch management etc. at the Cloud Site will be supported by the MSP for the entire contract period at no extra cost to department.
- MSP shall provide and implement tools and processes for monitoring the availability of assigned applications, responding to system outages with troubleshooting activities designed to identify and mitigate operational issues.
- MSP shall provide support for user registration, User ID creation, maintaining user profiles, granting user access, authorization, user password support, and support for print, file, and directory services.
- MSP shall document and perform patch management appropriate to the scope of their control and/or Provide self-service tools to perform patch management. Generate Alerts well in advance on the upcoming patches via email and management portal. All security patches and vulnerability fixes notified by nodal ministry must be done within 15 days of

3.2.3 *Self Service Management /Provisioning*

- Self Service management / provisioning focuses on capabilities required to assign services to users, allocate resources, and services and the monitoring and management of these resources.
- The MSP shall provide Self Service Provisioning Portal / Basic monitoring tool / Dashboard with two factors authentications via the SSL/TLS or SSH or through a web browser to remotely administer their virtual instances having fine-grained role-based access controls.

- It shall enable department to provision virtual machines, storage, and bandwidth dynamically (or on-demand), on a self-service mode or as requested.
- It shall enable service provisioning via online portal/interface (tools).
- It shall enable service provisioning via Application Programming Interface (API).
- It shall enable secure provisioning, de-provisioning and administering [such as Secure Sockets Layer (SSL)/Transport Layer Security (TLS) or Secure Shell (SSH)]
- It shall Support the terms of service requirement of terminating the service at any time (on- demand).
- It shall make the Management Reports described in this RFP accessible via online interface. These reports shall be available for one year after being created.
- The MSP shall ensure that effective Remote Management features exist so that issues can be addressed by department in a timely and effective manner.
- The MSP shall provide for automatic monitoring of resource utilization and other events such as failure of service, degraded service, etc. via service dashboard or other electronic means.
- The Utilization Monitoring tools shall have minimum following features:
    - Real time performance thresholds.
    - Real time performance health checks.
    - Real time performance monitoring and Alerts.
    - Historical Performance Monitoring.
    - Capacity Utilization statistics
- Cloud Resource Usage including increase / decrease in resources used during auto-scale The MSP shall provide Trouble Ticketing via online portal/ interface (tools).
- The MSP shall support maintenance of user profiles and present the user with his/her profile at the time of login.
- Audit trail of all administrative actions performed whether web portal or command line must be maintained for one year. All such audit trails should be encrypted through customer managed key and kept in isolated location (can be in CSP cloud as well), and must not be modified or deleted in any case. These can be archived/ deleted after 1 year, only after taking departmental approval. In case department wishes to retain them for longer period, MSP should provide the provision.
- These audit trails can be exported out of CSP and department can keep them in external system (outside CSP), such provision must always remain. Customer managed key for such data should be protected ad hand over to department post completion of the project.
- Instead of self-signed certificates, worldwide reputed CA certificates should be used with validity no longer than 2 years, for HTTPS communications.

3.2.4 *Data Management*

- The MSP shall strictly manage data isolation in the multi-tenant environment.
- The MSP should provide tools and mechanism to department (or its appointed agency) for configuring, scheduling, performing and managing back-ups and restore activities (when required) of all the data including but not limited to files, folders, images, system state, databases and enterprise applications in an encrypted manner as per the defined policy.
- MSP shall facilitate Transfer of data back in-house, either on demand or on termination of contract for any reason.
- MSP shall coordinate with the respective application owners and create data lifecycle policy wherever needed.
- MSP shall manage data reminisce throughout the data life cycle.
- MSP shall provide and implement security mechanisms for handling data at rest and in transit. Both data at rest and in transit should be encrypted.
- MSP must not delete any data at the end of the agreement (as per Exit Management Clause) without the express approval of department.
- When MSP (with prior approval of department) scales down the infrastructure services, MSP is responsible for deleting or otherwise securing content/data of the department prior to VM deletion and in case deleted, shall ensure that the data cannot be forensically recovered.

3.2.5 *User Administration*

- MSP shall Implement Identity and Access Management (IAM) that properly separates users by their identified roles and responsibilities, thereby establishing least privilege principles and ensuring that users have only those permissions necessary to perform their assigned tasks.
- MSP shall facilitate Administration of users, identities, and authorizations, effectively managing the root account, as well as any Identity and Access Management (IAM) users, groups, and roles they associated with the user account.
- MSP shall Implement multi-factor authentication (MFA) for the root account, as well as any privileged Identity and Access Management accounts associated with it for cloud portal.

3.2.6 *Help Desk*

- MSP must provide multiple support options catering to the varying levels of support requirements (e.g., toll free number, ticket, chat and forum) for the department.
- Department project manager shall be periodically visitingphysically/ virtually the data center site on quarterly basis or as and when required. MSP shall make convenient and secure provisions for at least 2 department personnel to access the department cloud infra and meeting with stake holder who all are providing the support service to department.

3.2.7 *Cloud Resource and Network Monitoring*

- MSP shall provision to monitor the network traffic in department cloud landscape.
- MSP shall provision to analyze amount of data transferred of each virtual machine.
- MSP shall provide network information of cloud virtual resources.
- MSP shall provision to monitor latency to cloud virtual devices from outside world.
- MSP shall provision to monitor network uptime of each cloud virtual machine.
- MSP shall provision for resource utilization i.e., CPU graphs of each virtual machine.
- MSP shall provision for resource utilization graph i.e., RAM of each virtual machine.
- MSP provision for resource utilization graph i.e., disk of each virtual machine. There shall be graphs of each disk partition and email alerts should be sent if any threshold of disk partition utilization is reached.
- MSP shall provision to monitor the uptime of cloud resources. The report shall be in exportable form.
- MSP shall provision tools to monitor the load of Linux/Windows servers and set threshold for alerts.
- MSP shall provision to monitor the running processes of Linux/Windows servers. This will help department to take the snapshot of processes consuming resources.
- MSP shall provision for setting alerts based on defined thresholds. There should be provision to configure different email addresses where alerts can be sent.
- MSP shall ensure that there should be historical data of minimum 6 months for resource utilization to resolve any billing disputes if any.
- MSP shall ensure that audit logs of scalability i.e., horizontal and vertical is maintained so that billing disputes can be addressed.
- MSP shall ensure that log of reaching thresholds used to trigger additional resources in auto provisioning are maintained.
- MSP shall ensure that there are sufficient graphical reports of cloud resource utilization and available capacity.
- MSP shall provide utilization reports for Internet bandwidth, load balancers etc.
- MSP shall provide ability monitor table space health and size.

- MSP shall provide ability to display live and waiting session.
- MSP shall provide ability of Monitoring and management of network link proposed as part of this solution.
- MSP shall provide ability to display monitoring parameters for continuous monitoring bandwidth utilization, latency, packet loss etc.

3.2.8 *Cloud Compute Requirements*

Provisioning of Virtual Machines (VM)

- The MSP shall do provisioning for required computing resources for hosting of all the required IT applications as listed. Virtual Machines shall be required to run the variety of workloads such as compute-intensive workload, memory-intensive workload, general- purpose workload, etc. The MSP shall deploy VMs on Server-Hardware having 1:2 Physical Core to vCPU ratio or 1:1 Ratio in case there is licenses cost saving without performance degradation
- CPU (Central Processing Unit) shall be provided with a minimum equivalent processor speed of 2.4GHz. The CPU shall support 64-bit operations.
- Department reserves the right to get the landscape audited by OEM, if deemed necessary.
- For SAP environment, MSP shall provision Virtual Machines only on SAP Certified Server hardware, if department deploy SAP workload.
- MSP shall deploy only SAP experience personnel for handling SAP based Virtual machine and related infrastructure if department deploy SAP workload.
- The virtual machine shall be capable of running different operating systems (Linux, Windows etc.) with any of their variants/ versions.
- Monitor VM up/down status and resource utilization such as RAM, CPU, Disk, IOPS and network.
- Department retains ownership of all virtual machines, templates, clones, and scripts/applications created for the department's applicationup until conclusion of exit management.
- Provide facility to configure virtual machine of required vCPU, RAM, and Disk.
- Provide facility to use different types of disks like SAS, SSD based on type of application.

3.2.9 *Administration, Configuration and Training*

- Upon deployment of virtual machines, the MSP has to assume full administrator access and is responsible for performing additional configuration, security hardening, vulnerability scanning, application installation, troubleshooting, hardening, patch/ upgrades deployment, BIOS and firmware upgrade as and when required.
- MSP shall ensure Preparation / Updating of the new and existing Standard Operating Procedure (SOP) documents on servers and applications deployment and hardening.
- MSP shall ensure Patching of VMs on the next available patch management change window and / or provide self-service tools to patch VMs.
- The MSP shall be setting up and configuring servers and applications as per configuration documents/ guidelines provided by department.
- The MSP shall do Installation/ re-installation of the server operating systems and operating system utilities in the VMs.
- MSP shall make provision to Monitor VM up/down status and resource utilization such as RAM, CPU, Disk, IOPS and network
- MSP shall monitor availability of the servers, MSP-supplied operating system and system software, and MSP's network.
- MSP shall ensure that VMs receive OS patching, health checking, Systematic Attack Detection, and backup functions.
- Monitor VM up/down status and resource utilization such as RAM, CPU, Disk, IOPS and network.
- MSP shall arrange training for 5 nos. department personnel on proposed cloud platform from OEM with certification.

3.2.10 *Internal Storage Requirements of VMs*

- The MSP shall provide scalable, redundant, dynamic Web-based storage.
- The MSP shall provide SSD based block storage capabilities with mandatorily IOPS stated in the BoQ Storage section, scalable per request for virtual machine instances of arbitrary size ranging from at least 1GB to 32TBs.
- The MSP shall provide options to use different types of disks based on performance requirement of the hosted application stack. Once mounted, the block storage should appear to the virtual machine like any other disk.
- MSP shall enable department to add either block storage volume or file level storage block to cloud VM from provisioning portal.
- There has to be different disk Space options to allocated for virtual machines and file data as per the requirement of department.

3.2.11 *Network Interfaces and Segmentation of VMs*

- MSP shall ensure that cloud VM network is both IPV4 and IPV6 compatible.
- MSP must ensure that cloud virtual machines are into separate network tenant and virtual LAN.
- MSP shall provide Private static IP addresses for all the VMs.
- MSP must ensure that all the cloud VMs are zoned in different network segments (VLANs) as per department requirements.
- MSP shall ensure the VMs provisioned should have minimum at least one of 10G vNIC and should be scalable to 25G each.
- MSP should ensure sub-millisecond latency between VMs within same data center.

3.2.12 *Security of VMs*

- VMs should be firewall protected
- The MSP shall provide Identity and Access Management for managing access to department users
- Hardening and patch management of underlying infrastructure by MSP
- Management of the OS processes and log files of the VMs
- Cloud service should support auditing with features such as what request was made, the source IP address from which the request was made, who made the request, when it was made, and so on.
- Management of the OS processes and log files including security logs retained in guest VMs.

3.2.13 *Server Load Balancing*

- Cloud service should deploy a Load Balancer to distribute the TCP, UDP, HTTP, HTTPs traffic across many computing resources within the same site to increase the responsiveness and availability of applications.
- Cloud service should provide secure, hardened, redundant (hardware or software) based Load balancer services.

3.2.14 *Backup/ Restoration / Migration / Deletion of VM Images and data*

- MSP shall provide the capability to copy or clone virtual machines for archiving, troubleshooting, and testing. It shall allow take an existing running instance (or a copy of an instance) and export the instance into a department's approved image format. Entire VM data backup must be available to department.
- MSP shall have provision for automatic restart (HA) of virtual machine on another physical server in case of host server failure.
- MSP shall have provision for live migration of virtual machine to any another physical servers or VM of any other cloud service provider (empaneled by MEITY) and vice versa irrespective of the location in case of predictive server failure. MSP shall perform an Image backup of department VM Image information or support the ability to take an existing running instance or a copy of an instance and export the instance into User department(s) required format.
- In case of suspension of a running VM, the VM shall still be available for reactivation for a one year without

having to reinstall or reconfigure the VM for the department solution. Beyond one year of suspension, all the data within it shall be immediately deleted / destroyed and certify the VM and data destruction to department as per stipulations and shall ensure that the data cannot be forensically recovered.

3.2.15 *Provisioning of Operating System and other Software*

- MSP shall provide adequate licenses for Operating system and other software (other than those in scope of department).
- MSP shall be able to support major Linux distributions – (Linux, Red Hat, SUSE, Ubuntu, Centos, and Debian etc.)
- MSP shall support latest Windows Server versions as per department requirements.
- MSP shall offer license portability of underlying department owned licenses having portability feature and support for Microsoft products etc.
- The virtual machine shall be capable of running different operating systems (Linux, Windows etc.) with any of their variants/ versions
- Software (limited to OS, security solutions and other platform stack offered by the MSP to department) will never be more than one version behind unless deferred or rejected by department. This is not applicable to software such as cloud management stack.

3.2.16 *Provisioning of Database Servers and DBA Services*

- MSP shall do provisioning for required Database Servers and Database administrator services for operating IT applications.
- CSP should have the provision of providing DB licenses installed on VMs (PostgreSQL & MS-SQL), as well as native managed databases (PostgreSQL, MySQL & MSSQL)
- The CSP should have the following SLA for the Native Managed Databases especially for PostgreSQL ,My-SQL & MS-SQL enterprise edition. The department may choose the managed databases based on the SLA for respective states or business urgency to optimize the cost for department e.g smaller state low priority may choose 99.95% SLA of database but larger state with critical database may choose 99.99% SLA to get the best ROI and availability of the system.
    - SQL Database with high availability (HA) >=99.95%
    - SQL Database Enterprise edition with high availability (HA)>=99.99%
- MSP shall offer the Database service that makes it easy to set up, operate, and scale a relational database in the cloud.
- Cloud service with Database server/ service should support a manual failover of the DB instance from primary to a standby replica.
- Cloud service with Database server/ service should support the needs of database workloads that are sensitive to storage performance and consistency in random access I/O throughput.
- Cloud service with Database server/ service should support creating multiple in-datacenter and across datacenter replicas within India per database instance for scalability or disaster recovery purposes.
- Cloud Service with Database server/ service should support enhanced availability and durability for database instances for production workloads.
- Cloud service with Database server/ service should support creating a DB back up and restoring the DB instance from the backup to a specific date and time.
- Cloud service with Database server/ service should allow monitoring of performance and health of a database or a DB instance.
- MSP shall perform following Database support services:
    - Installation, configuration, maintenance of the database (Cluster and Standalone).
    - Regular health check-up of databases.
    - Regular monitoring of CPU and Memory utilization of database server,
    - Alert log monitoring and configuration of the alerts for errors.
    - Space monitoring for database table space, Index fragmentation monitoring and rebuilding.
    - Performance tuning of Databases.

- Partition creation and management of database objects, Archiving of database objects on need basis.
- Patching, upgrade and backup activity and restoring the database backup as per defined interval.
- Schedule/review the various backup and alert jobs.
- Setup, maintain and monitor the 'Database replication' / Physical standby and Assess IT infrastructure up-gradation on need basis pertaining to databases.
- MSP shall perform following Database support services under the guidance of respective Application teams and their DBAs.

3.2.17 *Storage Provisioning*

- MSP shall do provisioning for required Storage for hosting of IT applications.
- MSP shall provide scalable, dynamic, and redundancy storage. MSP shall offer Block / File Object level storage to use with compute instances in the cloud.
- MSP shall provide storage management tools to cater dynamically scalable storage requirements of department.
- MSP shall have following storage offerings to address different kind of department's needs.
- CSP should provide high available (99.99%), reliable (99.9999%) storage.
- The application and database storage shall be provided on high-speed disks for better performance. MSP shall deliver disks with minimum 30 IOPS per GB for OLTP load/database & NFS file system. The IOPS for NON-OLTP workloads should be a minimum 6 IOPS per GB from Storage tier which support 64 TB per volume with 99.999% of volumes durability and Sub-millisecond latency performance storage tier. The CSP/MSP must ensure that BoQ Category for " Storage as a Managed Service - Block Storage" offers the required storage IOPS/ TB to meet the business requirements.
- MSP shall provide facility to use different types of disks like SAS, SSD based on type of application. Cloud service should offer SSD backed storage media to provide the throughput, IOPS, and low latency needed for a broad range of workloads.
- Cloud block storage should support consistent low latency performance at Sub-millisecond latency performance
- The application and database storage shall be provided on high-speed disks (minimum 3IOPS/GB) for better performance. MSP shall deliver disks with minimum 5IOPS per GB for OLTP load. The IOPS for NON OLTP load should be a minimum 3 IOPS per GB.
- MSP shall allow a minimum block of 1 GB to be provisioned by the department from self-service provisioning portal.
- The CSP should provide Archive Storage with milliseconds restore tier option for the data tiering and cost optimization
- Cloud service should support encryption of data on volumes, disk I/O, and snapshots using industry standard AES-256 cryptographic algorithm.
- Cloud service should support read after write consistency (each read and write operation is guaranteed to return the most recent version of the data).

3.2.18 *LAN Networking Requirements*

- MSP shall provide a redundant local area network (LAN) infrastructure and static IP addresses from customer IP pool or "private" non-internet routable addresses from MSP pool.
- Local Area Network (LAN) shall not impede data transmission.
- MSP shall deploy VMs in separate security zones / network isolation layers.
- Provide private LAN connectivity between primary DC and DR facilities.
- IP Addressing:
    - Provide IP address assignment, including Dynamic Host Configuration Protocol (DHCP).
    - Provide IP address and IP port assignment on external network interfaces.
    - Provide dedicated virtual private network (VPN) connectivity.

3.2.19 *IT Network Management Services*

- The MSP shall perform Monitoring and Management of network links proposed as part of this solution. The

MSP shall provide tools to monitor Bandwidth utilization, latency, packet loss etc.

- The MSP shall provide support in Call logging and co-ordination with vendors for restoration of links if need arises.
- The MSP shall provide support for Redesigning of network architecture as and when required by department.
- MSP shall give provision to monitor the network traffic of cloud virtual machine.
- MSP shall offer provision to analyze of amount of data transferred of each cloud virtual machine.
- MSP shall provide network information of cloud virtual resources.
- MSP shall offer provision to monitor latency to cloud virtual devices from its datacenter or from outside world.
- MSP must offer provision to monitor network uptime of each cloud virtual machine.

3.2.20 *Hardware Upgrades/ Software Updates / Patch Management*

- MSP shall perform patch management appropriate to the scope of their control and/or provide self-service tools to perform patch management. Any required version/Software /Hardware upgrades, patch management etc. at the Cloud Site will be done by the MSP for the entire contract period.
- Application Patch Updating will be done by department team.
- MSP shall Document all patch management related activities within the MSP's scope.
- The MSP shall ensure to Generate Alerts well in advance on the upcoming patches via email and management portal.

3.2.21 *Self Service Provisioning Portal*

- The solution should have ability to automatically provision services via a Web Portal (Self Provisioning), provide meter billing, to provide service assurance for maintenance and operations activities. Detailed user level or user group level auditing, monitoring, metering, accounting, quota, and show-back information is essential for the cloud platform to be offered.
- The Self-Service Provisioning Portal / Basic monitoring tool / Dashboard should have two factor authentications via the SSL/TLS or SSH or through a web browser to remotely administer their virtual instances having fine-grained role-based access controls.
- The MSP support team shall Interface with the technical team of MSP on behalf of department for all activities including monitoring the reports (e.g., usage, security, SLA,), raising (or escalating) tickets / incidents and tracking the same to resolution.

3.2.22 *Data Handling*

- To maintain confidentiality of department's data, MSP shall further ensure with an undertaking that the data cannot be forensically recovered after its deletion. The MSP should provide tools and mechanism to department or its appointed agency for configuring, scheduling, performing, and managing back-ups and restore activities (when required) of all the data including but not limited to files, folders, images, system state, databases, and enterprise applications in an encrypted manner as per the defined policy.
- The MSP shall manage data reminisce throughout the data life cycle. MSP shall not delete any data at the end of the agreement (for a maximum of 90 days beyond the expiry of the Agreement) without the express approval of department.
- The MSP shall provide mechanism to transfer data back in-house either on demand or in case of contract or order termination for any reason. On expiration/ termination of the contract, MSP shall handover complete data in the desired format to department which can be easily accessible and retrievable.
- All data in cloud should be backed up in such a manner that it can be restored either on-premises or in any other Meity approved CSP infrastructure. Department will randomly test restoration for different type of data (such as App, DB, file, block etc.) and only after that provide confirmation for data deletion on cloud. If there is any delay in providing such backup or technical issues in restoration which takes more than 90 days for department to confirm, charges by CSP for retaining data for additional days has to be borne by bidder.
- And only after confirmation from Dept (post successful restoration), all departmental data from CSP and MSP must be permanently deleted. This should be supported by an undertaking from bidder confirming the same.

3.2.23 *Monitoring Tools for MSP Services*

- MSP shall provide EMS/NMS solution for real-time monitoring of Network, Ips, subnet, Servers, Storage,

Uptime, Service status, and should be capable of reporting SLA violations.

- OEM support for the EMS proposed should be available throughout the contract period with access to software updates, maintenance patches and version upgrades.
- MSP shall provide solution to help department monitor RPO of each application in near real- time and RTO during DR drills.
- Provision tool should allow to configure the workflow of switchover/switchback.
- MSP shall implement tools that may analyse the resource utilization patterns and suggest the best practices for cost optimization

3.2.24 *REPORTS AND DOCUMENTATION*

MIS Reports

- MSP shall submit the reports on a regular basis in standard format. The following is only an indicative list of MIS reports that may be submitted.
- Daily
    - Summary of resolved unresolved and escalated issues / complaints
    - Log of backup and restoration undertaken
- Weekly
    - Summary of systems rebooted.
    - Summary of issues / complaints logged with the OEMs.
    - Summary of changes undertaken in the Data Centre including major changes like configuration changes, patch upgrades, etc. and minor changes like log truncation, volume expansion, user creation, user password reset, etc.

- Monthly
    - Availability reports of Servers / Virtual machines
    - Consolidated SLA / Non- conformance reports
    - Summary of component wise uptime
    - Log of preventive / scheduled maintenance undertaken
    - Log of break-fix maintenance undertaken
    - All relevant reports required for calculation of SLAs
- Quarterly
    - Consolidated component-wise availability and resource utilization
    - All relevant reports required for calculation of SLAs and verification of Invoices.
    - Logs and Audit Trails
    - Log Access Availability (what log file entries department has access to).
    - Log's retention period (the period during which logs are available for analysis).
    - Provide Audit Trail of the account activity to enable security analysis, resource change tracking, and compliance auditing.

3.2.25 *Alerts and Notifications*

- MSP shall offer a fast, flexible, fully managed push notification service that lets users send individual messages or to fan-out messages to large numbers of recipients.
- The MSP shall provide the infrastructure performance and availability of the cloud services being used, as well as alerts that are automatically triggered by changes in the health of those services.
- Event-based alerts, to provide proactive notifications of scheduled activities, such as any changes to the infrastructure powering the cloud resources.
- Notifications should be triggered each time a configuration is changed.

3.2.26 *Usage Reporting and Billing Management*

- Track system usage and usage reports.
- Monitoring, managing, and administering the monetary terms of SLAs and other billing related aspects.
- Provide the relevant reports including real time as well as past data/information/reports for the department to validate the billing and SLA related penalties. The reports shall consist of (not limited to) of:
    - Summary of resolved unresolved and escalated issues / complaints.
    - Logs of backup and restoration undertaken reports.

- Component wise Virtual machines availability and resource utilization reports.
- Consolidated SLA / Non- conformance reports.

Escalation Matrix and Team Member details

- The MSP shall provide updated escalation matrix either by email, at least once in a quarter or whenever there is a change in the escalation matrix whichever is earlier.
- The MSP shall also provide team member details for following teams:
  - Support Team
  - DR Drill Team

3.2.27 *Disaster Recovery Services*

Overview

- MSP is responsible for Disaster Recovery Services so as to ensure continuity of operations in the event of failure of primary data center. MSP shall design and document an efficient disaster recovery solution in lines with the requirements of department and as per the RPO and RTO requirements.
- The solution should be architected to run on cloud services to provide business continuity with no interruptions in case of any disruptions /disaster at DC through automated processes of redirecting the department data traffic to DR site.
- During normal operations, the Primary Data Centre 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 as per the solution offered.
- The application environment shall be installed and ready for use.
- The MSP should offer switchover and switchback of individual Servers / VMs/Applications /Components instead of entire system.
- Till a disaster (planned/ testing or otherwise) is declared by department the users should not be allowed to access the IT applications from DR site (or as per discretion of department).
- Application team should support DR switch over for applications / architecture that do not have automatic switch over capabilities.

RPO and RTO Requirements

- The service parameters to be met by the DR system focus on the Recovery Time Objective (RTO) and the Recovery Point Objective (RPO), which in business terms define the 'Interruption to Service' and 'Loss of Data' respectively. The RTO will be calculated from the time of "declaration of a disaster" up to the time by which all the applications are made fully operational and end users are able to access these applications and carry out the business operations.
- RPO:RTO = 15 min:180 min for the DR (Disaster Recovery)
- The MSP should offer a dashboard to monitor RPO and RTO of each data type.

Replication Requirements

- MSP shall adequately do the sizing of DC-DR replication links and commission them with (1+1) redundancy, to meet the RTO and the RPO requirements.
- DR Transactional Databases 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. There shall be asynchronous replication of data between Primary DC and DR. Any lag in data replication should be clearly visible in dashboard and alerts of same should be sent to department.
- MSP shall be responsible for providing/facilitating replication tools / software/ processes for Databases, Active Directory, Web Servers, application etc. for seamless replication from DC to DR and vice versa to meet RPO and RTO requirements.
- MSP shall provide detailed operating manuals for replicating these solutions.
- The MSP shall deploy these tools after acquiring consent from department's project in charge.
- The MSP shall provide details of replication mechanism for (but not limited to) the following solutions:
    - Operating system
    - Database
    - Application server
    - File server
    - Email server
    - Active Directory/LDAP

DC-DR Failover and Restoration – Mock Drills / Actual Disaster

- The MSP shall also clearly specify the situations in which disaster shall be announced along with the implications of disaster and the time frame required for complete switchover to DR.
- The failover from primary DC to DR should be done through a proper DR announcement process which should be documented as part of BCP planning. In the event of a disaster, the system at proposed MSP's DR Data Center will be primary system.
- The DR should be available (with its data) on-demand basis within the defined RTOs and RPOs, wherein 100% of the services of DC would run from DR site. All users of department will connect to MSP's system through Internet link.
- During the drill, the MSP shall demonstrate the fulfilment of SLAs at load of 100% users with 60% concurrency.
- The use of Full Compute DR environment can be for specific periods during a year for the purposes of DC failure or DR Drills or DC maintenance.
- Application data and application states will be replicated between data centers so that when an outage occurs, failover to the surviving data center can be accomplished within the specified RTO. The installed application instance and the database shall be usable.
- During the change from DC to DRC or vice-versa (regular planned changes), it should be as per the given RPO.MSP shall provide workflow-based switchover/ failover facilities (during DC failure and DR Drills). The switchback mechanism shall also be workflow based. The MSP shall also provide a tool/ mechanism for

- Department to trigger DR switchover, for example a “one-click DR”wherever the application / architecture supports. MSP shall provide support for the development and configuration of any additional scripts for successful working of DR along with support from application team.

- The Database and storage shall be of full capacity and the licenses and security shall be for full infrastructure. The bandwidth at the DR shall be scaled to the level of Data center. Users of application should be routed seamlessly from DC site to DR site.

- Restoration provides an easy process for copying updated data from the DR server back to the DC server. Whenever main DC will be recovered and operational, the data from DR system to DC systems should be synchronized. Once this data is synchronized and verified, the switchover from DR system to DC system should be done. In that case all users will be accessing systems of main DC.

- MSP shall provide detailed DR activity plans which will contain steps/procedures to switch over services to DR site in the event of invocation of disaster at DC site.

- MSP shall also document steps for restoring services from DR site to DC site.

- In case of failover to DR site (once disaster is declared) within the defined RTO, the SLA would not be applicable for RTO period only. Post the RTO period, SLA would start to apply and should be measured accordingly.

- The MSP shall conduct DR drill for one month at the interval of not more than six months of operation wherein the Primary DC has to be deactivated and complete operations shall be carried out from the DR Site. The pre-requisite of DR drill should be carried out by MSP and department jointly. The exact process of the DR drill should be formulated in consultation with the department team in a way that all elements of the system are rigorously tested, while the risk of any failure during the drill is minimized. The process should be documented by the MSP as part of the disaster recovery plan. MSP shall plan the activities to be carried out during the mock drill and issue a notice to the department at least 15 working days before such drill.

- During the DR drill, the MSP need to arrange the full DR team with sufficient resources and expertise and complete the activity under the supervision of senior resource for co- ordination. The MSP shall develop appropriate policy, checklists in line with ISO 27001 and ISO 20000 framework for failover and fall back to the appropriate DR site.

3.2.28 *DR Managed Services*

- Provision for managed services for the entire DR facility will be required. MSP shall provide continuous maintenance activities to support the disaster recovery site. This includes (but not restricted to):

- MSP shall provide support for all server maintenance activities. This would include periodic health check, on-demand troubleshooting, repairs, part replacement etc. from certified vendors. ITIL processes named problem, change, incident and configuration will be followed by MSP at DR site.

- MSP should have proper escalation procedure and emergency response in case of failure/disaster at DC.

- MSP may partner with respective application / product support vendor to support DR in event of disaster or for performing periodic maintenance and upgrade activities

- MSP shall perform RPO monitoring, reporting and event analytics and other activity

associated with operations and management of DR plan and Implementation for the disaster recovery solutions.

- MSP shall provide a monitoring tool with dashboard showing RPO, RTO, changeover facility etc.
- The date, time, duration, and scope of each drill shall be decided mutually between department and the MSP. Extreme care must be taken while planning and executing DR drills to ensure that there is no avoidable service interruption, data loss, or system damage at DC.
- To demonstrate how the application fails over when the primary site goes down. The testing should include the:
    - Uninterrupted replication to DR servers.
    - Lag in replication due to any unforeseen errors.
    - Process of recovering from lags if any.
    - Data integrity test of DR servers.
- The MSP shall be responsible providing input for
- Devising and documenting the DR policy discussed and approved by department.
- Providing data storage mechanism with from the Go-Live date till the date of contract expiry for the purpose of compliance and audit.
- MSP shall support in bringing the machines to login level in case of disaster / DR drills. Provisioning, configuring, and managing FC-IP router for DC to DR replication in case the proposed solution requires FC-IP router.
- The solution is envisaged for application-level recovery scalable to site level recovery based on the impact of the disaster.
- In case of reverse replication, since the DR site would be acting as main site, all the necessary support to run the environment has to be provided by the MSP.
- Reverse Replication is necessary and envisaged when the DR site is acting as the main site. The solution should ensure consistency of data in reverse replication till the operations are not being established at the Cloud site. The RPO would be applicable in reverse replication also. The entire data should be made available for restoration at Primary Data Centre.

3.2.29 *Business Continuity Planning*

- MSP shall define and submit (as part of the solution), a detailed approach for “Business Continuity Planning”; this should clearly delineate the roles and responsibilities of different teams during DR Drills or actual disaster; further, it should define the parameters at which “disaster” would be declared.
- The MSP should have a practicing framework for business continuity planning and the plan development for which has been established, documented, and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements.
- The MSP should practice Business continuity and security incident testing at planned intervals or upon significant organizational or environmental changes.

- Incident response plans should be developed by the MSP and executed by MSP, application provider and department which should involve impacted customers (tenant) and other business relationships that represent critical intra-supply chain business process dependencies.

3.2.30 *Backup and Restore Service*

- MSP shall provide backup solution for application/ architecture supports backup, covering but not limited to 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.
- MSP shall cover (not limited to) Backup and Restoration of VM images, Operating System, Applications, Databases and File system etc.
- MSP shall Configure, schedule, monitor and manage backups of all the data including but not limited to files, images, and databases as per the policy/procedure/plan finalized by department.
- MSP shall also perform Administration, tuning, optimization, planning, maintenance, and operations management for backup and restore.
- MSP should propose cloud native solution or use a SaaS based/Third Party Software deployed on VM based backup software.
- The Long-Term Storage should have an option of enforcing WORM (Write Once, Read Many) policy for section of data that requires the same.
- The backup service should support granular recovery of virtual machines, database servers, Active Directory, etc.
- Department should be able to recover individual files, complete folders, entire drive or complete system to source machine or any other machine available in network.
- MSP shall Provide and install additional infrastructure capacity for backup and restore.
- There has to be provision if required to shift the backup at department required location on tape/USB.
- MSP shall perform restoration testing biannually with the permission of department.
- MSP must ensure integrity of the data returned during a restore by verifying the block data read with a check sum of the data.
- MSP shall ensure prompt execution of on-demand backups and restoration of volumes, files and database applications whenever required.
- MSP shall perform 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.
- The backup service must provide following capabilities.
- Compression: Support compression of data at source before backup
- Encryption: Support at least 128-bit encryption at source
- Alert: Support email notification on backup job’s success / failure
- File exclusion: Ability to exclude specific files, folders, or file extensions from backup

- Deduplication: Provide deduplication capabilities
- Backups should be stored in such a way that disaster at either DC or DR or both should not result in loss of backups.

#	Backup Type	Backup Frequency	Retention Period
1	Incremental	Daily	14 Days
2	Full	Weekly	45 Days
3	Full	Monthly	12 Months
4	Full	Yearly	7 Years

#	Restoration Policy	
1	Backup taken in last month	Once in a Month
2	Backup taken in last quarter	Once in a Quarter

3.2.31 *Exit Management / Transition-Out Services*

- Continuity and performance of the Services at all times including the duration of the agreement and post expiry of the Agreement is a critical requirement of department. It is the prime responsibility of MSP during exit management period and in no way any facility/service shall be affected/degraded. Further, MSP is also responsible for all activities required to train and transfer the knowledge to department (or representative agency of department).
- 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 MSP. The exit management period ends on the date agreed upon by department or Three months after the beginning of the exit management period, whichever is earlier.
- At the end of the contract period or upon termination of contract, MSP is required to provide necessary handholding and transition support to ensure the continuity and performance of the services to the complete satisfaction of department.

Exit Management Plan

- MSP shall provide department with a recommended “Exit Management SOP” 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.
- MSP shall provide support to department for transferring data / applications at the time of exit management and as per the guidelines defined by MeitY in Cloud Services empanelment RFP.
- Exit Management Plan will include following but limited to:

- 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.
- Plans for the communication with such of the MSP, 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.
- Plans for provision of contingent support to the implementation of IT Infrastructure Solution for a reasonable period (minimum one month) after transfer.
- Method of Transition including roles and responsibilities of both the parties to handover and takeover the charge of project regular activities and support system.
- Proposal for necessary setup or institution structure required at department level to effectively maintain the project after contract ending.
- Training and handholding of department Staff or designated officers for maintenance of project after contract ending.

- Department will approve this plan after necessary consultation and start preparation for transition.

Exit Management Services

- MSP shall be responsible for copy all data, scripts, software, virtual machine images, and so forth to enable mirroring or copying to department supplied industry standard media.

- MSP shall retain the data / copy of Database for 90 days and MSP shall ensure that there is no deletion of data for a minimum 90 days beyond the expiry of the contract without any confirmation from department. If data is to be retained beyond 90 days, the cost for retaining the data may be obtained in the commercial quote.

- The format of the data transmitted from the MSP to the department should leverage standard data formats (e.g., OVF, VHD…) whenever possible to ease and enhance portability. MSP must ensure that the virtual machine format is compatible with other MSP, so that department can migrate from one MSP to other MSP. Department should be able to export the virtual machine from MSP cloud and use that anywhere. MSP shall give provision to import cloud VM template from other MSPs.

- MSP shall necessarily support for /establishment of network connectivity to / from other MSPs (within India) if required

- MSP shall ensure that all the documentation required by the department for smooth transition (in addition to the documentation provided by the MSP) are kept up to date and all such documentation is handed over to the department during regular intervals as well as during the exit management process. Also ensure that all the documentation required for smooth transition including configuration documents are kept up to date

- Post exits all the data content should be removed to ensure that the data cannot be recovered.

- MSP shall address and rectify the problems with respect to migration of the department

- application and related IT infrastructure during the transition.

- MSP shall decommission and withdraw all hardware and software components after the

completion of the contract period and formally close the project. This process will be initiated 6 months before the ending of the project contract.

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

- Payments during the Exit Management period shall be made in accordance with the Terms of Payment Schedule.

3.2.32 *Connectivity and Customer Premises Equipment features*

WAN Connectivity Requirements

- MSP shall provide end-to-end MPLS connectivity for the DR Site.

- MSP has provided redundant internet link in primary and DR site to access the application from department office and other locations.

- MSP shall provide dedicated private connectivity from Department (to be specified by Department) to nearest CSP edge location for the use of large data transfer. All other office locations may be connected through site-to-site VPN over IPSEC.

- MSP has to configure the network links in auto failover mode is the responsibility of the MSPs.

- Identification and classification of at least the following classes of application types must be supported by the solution:

    - Client server and web-based applications

    - Antivirus Solution

    - Operating System and Client software patching solution

- The vendor should ensure that traffic is prioritized as per the listing given by department. The actual division could change over time as per requirement of department Vendor should be able to make changes as required by department.

- MSP shall have provision of secure tunnel / links for data replication to provide secure data replication for DR services.

- MSP shall provide Managed Anti-DdoS Services capable of handling at least 1 GB of DdoS Attacks in all the links.

- MSP shall provide ‘Clean Pipe’ in all the links.

- MSP shall provide 24 x 7 x 365 Service Window for Link Management Services. The support mechanism must be confirmed by the MSP with response times.

- The MSP shall assign a service manager for the duration of the Contract this resource should be the “Single point of contact” for all service-related matters for department and should be able to respond within the designated service window. The proposed “Service manager” should be a multi-skilled professional and supported by back-end support as required.

- The proposed solution should also provide self-service capabilities which gives configuration access to department team.
- MSP shall be responsible for DNS / reverse DNS changes in the Internet connectivity as and when required.
- MSP should provide a report based on the IP and application high consumption bandwidth

3.3. Cloud Security Requirement

The MSP should ensure complete security requirements for the Cloud hosting of department with suitable security arrangements through SaaS model (Security as a Service) as per MeitY guidelines. MSP shall provide end-to-end security services to meet IT security challenges for the infrastructure based on the proven frameworks and security best practices. It is vital for complete security that the processes and technology which shall support the Information Security function are proven and adhere to standards.
It is envisaged that the security operations shall be centralized, structured, and coordinated and shall be responsive resulting in effective threat prevention and detection helping the deployed cloud solution to be secure from attackers. The Information Security functions shall respond faster, work collaboratively, and share knowledge more effectively. The proposed cloud solution shall have multiple security layers to secure the infrastructure from threats. MSP shall propose and provide security solutions that may not be mentioned in the RFP but are required as per the guidelines of MeitY.
MSP shall provision for following security solutions (not limited to):

- CSP Native Next-Generation Firewall (NGFW) having minimum 2 Gbps threat-prevention throughput (all features enabled).
- Web Application Firewall for OWASP Top 10 protection
- IPS and IDS separate service on-demand billing on the CSP Portal
- Malware Analysis – MSP shall conduct analysis of newly discovered malware to uncover its scope and origin.
- DdoS service – MSP would offer DDOS Protection to protect the cloud infrastructure and application from well-equipped attackers. Minimum mitigation of 1 Gbps.
- Anti-Virus – This Service includes virus detection and eradication, logon administration and synchronization across servers, and support for required security classifications.
- IAM – The User Management services shall include Directory Services for which comprises of the following services:
    - Domain management
    - Group management
    - User management
    - Implementation of domain policies and standards etc.
    - Directory services are to be used by department.
    - Role Management
    - Access Management

- Multi-Factor Authentication
- Best practices from enterprise security including password strength, password aging, password history, reuse prevention etc. must be followed for access control.

- SIEM – The MSP shall also propose for Security Information and Event Management (SIEM) solution supporting threat detection and security incident response through the real-time collection and historical analysis and correlation of security events from a wide variety of event and contextual data sources. It shall also support compliance reporting and incident investigation through analysis of historical data from these sources.

- VAPT – The MSP shall conduct vulnerability and penetration test (from a third-party testing agency which has to be CERT-IN empaneled) on the Cloud facility every 6 months and reports shall be shared with department. The MSP needs to update the system in response to any adverse findings in the report, without any additional cost to department.

- Security solution during data in transit and at rest

- NTP (Network Time Protocol) – Clock Synchronization – The provisioned NTP solution should have the capability to synchronize clock with systems like network equipment, voice systems, servers, appliances, desk top systems etc.

It is critical to have a set of IT security management processes and tools to ensure complete security of cloud solution. An IT security policy, framework, and operational guidelines as per ISO 27001, 27017, 27018 and PCI-DSS be maintained and implemented by Cloud service provider (MSP).
Department will perform physical audits at the Data Centre and will require access to the department's infrastructure as and when required by department.
All the security management processes, tools and usage shall be well documented in security policy and the security best practices to be followed to maintain IT security.
Data shall not leave the Indian boundaries and data residing within Cloud shall not be accessed by any entity outside the control of department.
Cloud service shall support audit features such as what request was made, possibly the source IP address from which the request was made, who made the request, when it was made, and so on.

Security Controls
MSP shall provide adequate security controls not limited to the measures as described below:

- Secure Access Controls
  - The system shall include mechanisms for defining and controlling user access to the operating system environment and applications. Best practices from enterprise security including password strength, password aging, password history, reuse prevention etc. must be followed for access control.

- Authorization Controls
  - A least-privilege concept such that users are only allowed to use or access functions for which they have been given authorization shall be available.

- Logging

- Logs must be maintained for all attempts to log on (both successful and unsuccessful), any privilege change requests (both successful and unsuccessful), user actions affecting security (such as password changes), attempts to perform actions not authorized by the authorization controls, all configuration changes etc. Additionally, the access to such logs must be controlled in accordance with the least privilege concept mentioned above, so that entries may not be deleted, accidentally or maliciously.

- Hardening
  - All unnecessary packages must be removed and/or disabled from the system. Additionally, all unused operating system services and unused networking ports must be disabled or blocked. Only secure maintenance access shall be permitted, and all known insecure protocols shall be disabled.

- Malicious Software Prevention
  - Implementation of anti-virus software and other malicious software prevention tools shall be supported for all applications, servers, data bases etc.

- Network Security
  - The network architecture must be secure with support for UTM, Firewall and encryption. The system shall also allow host-based firewalls to be configured, as an additional layer of security if the network firewall were to fail.
  - Cloud services shall be provided on a 10Gbps scalable to 50Gbps network connectivity between the server and Storage and Network. Cloud service shall be able to support multiple (primary and additional) network interfaces. The proposed data center shall be isolated from failures in other data centers. As mentioned in RFP, MSP's proposed Data Centre shall be connected with low latency and in-expensive network connectivity.
  - Cloud service provider should be able to configure the secure network over an internet like Ipsec VPN tunnel or SSL VPN.
  - Cloud services shall provide a web interface with support for multi-factor authentication to access and manage the resources deployed in cloud and also provide Audit Trail of the account activity to enable security analysis, resource change tracking, and compliance auditing.

- Information Security: Log Monitoring and Correlation

- All Servers / sub systems / network devices / appliances as proposed shall have capability and throw logs to the log server. The Logs and events generated by VMs, applications, DB, network, security component / devices of the system shall be monitored. MSP must provide a Security information and event management (SIEM) solution for the same which shall be capable to provide various security alerts, events, logs generated from various IT infrastructure (Hardware/Software) components. MSP would need to ensure the IT security compliance and therefore monitor the threats/logs generated by various equipment's / sub systems.

- Minimum 500 EPS with storage capacity for storing the event for minimum 6 months. Also, MSP will be required to scale the storage if the existing storage space is full.

Cloud Security Administration

The MSP shall provide 24x7x365 managed services for the entire security stack protecting the department environment. MSP shall be responsible for managing configuration and patch management, vulnerability scanning, protecting data in transit and at rest, managing credentials, identity, and access management etc. The activities include:

- Cloud Security Posture Management (CSPM) support multi-clouds
- Cloud Workload Protection Platform (CWP)
- Appropriately configure the security groups in accordance with the Security policies
- Regularly review the security group configuration and instance assignment in order to maintain a secure baseline.
- Secure and appropriately segregate / isolate data traffic/application by functionality using DMZs, subnets etc.
- Ensure that the cloud infrastructure and all systems hosted on it, respectively, are properly monitored for unauthorized activity
- Conducting regular vulnerability scanning and penetration testing of the systems, as mandated by their Government Agency's policies
- Review the audit logs to identify any unauthorized access to the government agency's systems.
- The protection from unauthorized usage, detection of intrusions, reporting as required and proactive prevention actions are to be provided by MSP.
- Service Component Administration
- User and Password Control
- Check and maintain access control
- Routine connection tests
- Change and Configuration Management
- IP / Port / Zone Configuration
- Firewall policy / Ipsec VPN / SSL VPN configuration
- NAT / PAT configuration
- Multicast configuration
- Antivirus / IPS Signature update, when released by vendor
- Fault Management
- Response to alerts generated by systems or problems reported.
- Troubleshooting, root cause analysis (RCA) and identification of problem area
- Resolution of problems through configuration changes/ re-installations / replacements
- Escalate hardware failures to hardware vendor
- Assist hardware vendor to Identify problem area (by log collection and reboot)
- Log Storage: Store critical logs in shared Syslog server for retention period of 90 days
- Configuration backup: Take incremental configuration backup daily for retention period of 90 days and Restoration of configuration when required.

- Trouble ticket logging, update, and closure
- Managing configuration and security of Demilitarized Zone (DMZ) Alert / advise department about any possible attack / hacking of services, unauthorized access / attempt by internal or external persons etc.
- Incident Response – The MSP should have policies and procedures in place for timely detection of vulnerabilities within organizationally owned or managed applications, infrastructure network and system components (e.g., network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. The MSP/MSP must also have policies and procedures in place to ensure timely and thorough incident management, as per established IT service management policies and procedures. The Solution shall be complied with ITIL (Information technology Infrastructure library) standards.
- Governance and Risk Assessment – The MSP should have organizational practices in place for policies, procedures and standards for application development and service provisioning as well as design, implementation, testing, use, and monitoring of deployed or engaged services in the cloud.

3.4. MSP Technical and Functional Compliance for Cloud Services

Cloud Services Capabilities

Sr.	Cloud Capabilities	Compliance(Y/N)
1	In order to increase the service availability, the cloud service provider must offer multidimensional auto-scaling of cloud services where resource like RAM and CPU will scale vertically as well systems should scale horizontally	
2	Cloud service should enable to provision cloud resources through self service provisioning interface.	
3	Cloud System should enable to provision cloud resources from application programming interface (API)	
4	Cloud System should be accessible via secure method using SSL certificate.	
5	Should be able to create, delete, shutdown, reboot virtual machines from Cloud portal.	
6	Should be able to size virtual machine and select require operating system when provisioning any virtual machines	
7	Should be able to predict billing of resources before provisioning any cloud resources if integrated with billing system.	
8	Should be able to set threshold of cloud resources of all types of scalability.	
9	Should be able to provision any kind of resources either static or elastic resources.	
10	The cloud virtual machine created by portal should have at-least two virtual NIC cards. One NIC card should be used for internet traffic while other should be used for internal service traffic.	
11	The Cloud System shall be capable of allowing applications to self-service compute, network and storage infrastructures automatically based on workload demand.	
12	Should ensure that the virtual machine format is compatible with other cloud systems.	
13	Cloud System should give provision to import cloud VM template from other cloud systems.	
14	Cloud System should support provisioning from self-Cloud Orchestration System to add more storage as and when require by VM.	
15	Cloud System should give provision to attached new block disk to any cloud VM from self-service portal.	
16	The cloud virtual machines should be scalable in terms of RAM and CPU automatically without reboot.	
17	Cloud System must support multi-tenancy for management perspective.	

	Different department or group company should be able to access allocated resources only.	
18	The Solution should provide a simple to use intuitive web end experience for Cloud Administrator and User Departments.	
19	The Solution should provide Unified Infrastructure management with complete inventory management of virtual machines and physical resources.	
20	The Solution should provide comprehensive service catalog with capabilities for service design and lifecycle management, a web-based self-service portal for users to order and manage services.	
21	Cloud System should have provision to ensure that cloud virtual machine is into separate network tenant and virtual LAN.	
22	Cloud System must ensure that cloud virtual machines are having private IP network assigned to cloud VM	
23	Cloud System must ensure that cloud virtual machines are having private IP network assigned to cloud VM.	
24	Cloud System must ensure the ability to map private IP address of cloud VM to public IP address as require from portal of Cloud Orchestration System.	
25	Should ensure that cloud VM network is IPV6 compatible.	
26	Should support use of appropriate load balancers for network request distribution across multiple cloud VMs.	
27	Cloud Orchestration System should provide network information of cloud virtual resources.	
28	Cloud Orchestration System should have built-in user-level controls and administrator logs for transparency and audit control	
29	Cloud System should support policy-based provisioning of virtual machines. Based on granted permission, users should be able to perform the operations. For example, if any users don't have permission to delete VM, he should not be able to do it.	
30	Cloud System should support quota-based system. Users should not be able to provision resources beyond allocated quota.	
31	The admin should be able to define Access Control to Permit or Deny operation per Group or per User.	
32	Should have provision to define Workflow to Escalate Permission to Group Admins or System Admins.	
33	The Solution should allow for implementing workflows for provisioning, deployment, Decommissioning all virtual and physical assets in the cloud datacenter.	
34	User Management: The solution shall provide comprehensive user management	
35	Functions including tenant-specific user grouping and admin/user rights within the scope of a tenant. The tenant-admin user is considered distinct from the overall cloud solution administrator. The tenant-admin shall be able to manage own profile, tenant preferences, as well as users within the tenant/group scope. Individual users shall be able to manage their own profile and individual preferences. The solution administrator shall have the rights to all User Management functions.	

36	Cloud System should provide facility to make template from virtual machines.	
37	Cloud System should give provision to make clone of cloud virtual machine from Cloud Orchestration System.	
38	Cloud System should have provision to live migration of virtual machine to another physical servers in case of any failure.	
39	Cloud System should have provision to migration of virtual machine from one hypervisor platform to another hypervisor platform through its UI.	
40	Cloud System cloud shall continuously monitor utilization across Virtual Machines and shall intelligently allocate available resources among the Virtual Machines.	
41	The Cloud System solution shall be able to dynamically allocate and balance computing capacity across collections of hardware resources of one physical box aggregated into one unified resource pool.	
42	The Cloud System cloud solution should support detecting, in real time, resource requirements of a system in virtual environment and automatic scaling of resource parameters like RAM and CPU to compensate resource requirement in a system.	
43	The solution shall provide near zero downtime host patching with maintenance mode to move running workloads to other hosts on the platform with a consistent audit trail of the patching process.	
44	Cloud System should give provision to monitor the network traffic of cloud virtual machine.	
45	Cloud System should offer provision to analyses of amount of data transferred of each cloud virtual machine.	
46	Cloud System must offer provision to monitor uptime of each cloud virtual machine.	
47	Cloud System 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.	
48	Cloud System must make provision of resource utilization i.e., CPU graphs of each cloud virtual machine.	
49	Cloud System must make provision of resource utilization graph i.e., disk of each cloud virtual machine. There should be graphs of each disk partition and emails should be sent if any threshold of disk partition utilization is reached.	
50	Cloud System must give provision to monitor the load of Linux/Windows servers and set threshold for alerts.	
51	Cloud System must ensure that there should be historical data of minimum 6 months for resource utilization in order to resolve any billing disputes if any.	
52	Cloud System must ensure that there are sufficient graphical reports of cloud resource utilization and available capacity	
53	Should be able to create virtual instances of required configuration without limiting to any standard templates	

General Cloud Requirement

Sr. No	Name of Service	Specification	Compliance(Y/N
1	Security Monitoring and Posture Management	The CSP should have a Managed service for a comprehensive view of the high-priority security alerts and compliance status across multiple accounts.	
		Managed service to provide a single place that aggregates, organizes, and prioritizes the security alerts, or findings, from multiple services and sources.	
		The findings should be visually summarized on integrated dashboards with actionable graphs and tables.	

		CSP should have capability to continuously monitor the environment using automated compliance checks based on the best practices and industry standards.	
2	Identity and Access Management	The CSP should have capabilities to securely control access to services and resources for the users.	
		CSP should have abilities to create and manage users.	
		CSP should have capabilities to create roles and groups.	
		Support to enforce permissions-based access to the resources.	
		Support to manage federated users and their permissions.	
3	Threat Detection	The CSP should offer a fully managed threat detection service.	
		Capabilities to continuously monitor for malicious or unauthorized behavior.	
		Capabilities to analyze billions of events across multiple accounts using machine learning to detect anomalies.	
		The threat detection service should be able to generate actionable alerts.	
		The threat detection service should support integration with existing event management and workflow systems.	
4	Security Assessment Services	The CSP should offer a service for automated security assessment.	
		Service to help improve the security and compliance of applications deployed on the cloud.	
		Managed service to automatically assess applications for exposure, vulnerabilities and deviations from best practices.	
		Service should be able to produce a detailed list of security findings prioritized by level of severity.	
		Should be able to check for unintended network accessibility and vulnerabilities of the VMs.	
		Rules should be regularly updated by the CSP.	
5	SSL Certificate	The CSP should have a service to provision, manage, and deploy Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates.	
6	Firewall Management	The CSP should offer a security service to centrally configure and manage firewall rules.	
		The security service should be able to configure firewall rules across multiple accounts and applications.	
		The security service should provide a mechanism to easily roll out firewall rules.	
		The security service should be able to support new applications and resources into compliance with a common set of security rules from day one.	
		The security service should provide a single place to build firewall rules, create security policies, and enforce them in a consistent, hierarchical manner.	

7	Encryption Key Management	The CSP should offer a fully managed service to create and manage encryption keys.	
		fully managed key management service should be able to control encryption across a wide range of cloud services and applications.	
		fully managed key management service should be FIPS 140-2 complaint.	
		fully managed key management service should be able to provide the logs of all key usage to help meet our regulatory and compliance.	
8	Password Management	The CSP should have a fully managed service to centrally manage secrets needed to access the applications, services, and IT resources.	
		fully managed secret management service should be able to easily rotate, manage and retrieve database credentials, API keys, and other secrets throughout their lifecycle.	
		fully managed secret management service should be able to support API based retrieval of secrets.	
		fully managed secret management service should be able to control access to secrets using fine-grained permissions.	
		fully managed secret management service should be able to audit secret rotation centrally for resources in the cloud, third-party services and on-premises.	
9	DDoS Protection	The CSP should have a managed service to protect against Distributed Denial of Service (DDoS) attacks.	
		Managed DDoS protection service should provide always-on detection and automatic inline mitigations that minimize application downtime and latency.	
10	Single Sign-On	The CSP should have support for Single Sign-On (SSO).	
		The SSO service should be able to centrally manage SSO access to multiple accounts and business applications.	
		The SSO service should be highly available.	
		The SSO service should support built-in SAML integrations to many business applications.	
		The SSO service should be able to extend SSO access to any of the SAML-enabled applications.	
		The SSO service should be able to use existing corporate credentials to access all the assigned accounts and applications from one place.	
11	Web Application Firewall	The CSP should have a managed web application firewall.	
		The web application firewall should be able to protect the web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources.	
		The web application firewall should be able to give us control over which traffic to allow or block the web application by defining customizable web security rules.	

		The web application firewall should support creation of new custom rules and block common attack patterns, such as SQL injection or cross-site scripting, OWASP's Top 10 Web Application Vulnerabilities and rules that are designed for our specific application.	
		The web application firewall should be able to deploy new rules immediately.	
		The web application firewall should support API based operations to automate the creation, deployment, and maintenance of web security rules.	
12	Multi-factor authentication	The CSP should offer rule based multi-factor authentication for the cloud portal.	
13	Automated Vulnerability Management	The CSP should offer automated vulnerability management service that continually scans virtual machines and container workloads for software vulnerabilities and unintended network exposure.	
		The CSP managed Vulnerability Management Service should automatically detect all newly launched Virtual Machines, and container images pushed to container registry and immediately scans them for software vulnerabilities	
		The CSP managed Vulnerability Management Service should perform automated discovery and continual scanning that delivers near real-time vulnerability findings	

Cloud Portal Service Provisioning

S No	Eligibility Criteria	Compliance(Y/N
1	Secured, authenticated and authorized Service APIs to Provision/Scale/Manage the resources	
2	Public Documentation of every API along with examples available in popular programming languages including CLI, Java, Python, Node.js etc.	
3	Metering and Monitoring of Service usage in terms of compute, bandwidth, storage, performance metrics	
4	Security by Design: Encryption of data at Rest and while Transit enabled without any manual configuration required. The TLS certificates and Encryptions keys should be secured by Key Management Solution backed by HSM.	
5	Integration with CSP Identity and Access Management (IDAM) solution to allow granular access control.	
6	Automated Backup of data with IDAM based Access Control, encryption and monitoring for access/download.	
7	Automatic Failover without manual intervention.	
8	Self-Service capability for Restoration of cluster from backup.	
9	Self-heal capability to detect health of underlying hardware and restore services on a different physical host without any manual intervention.	
10	Integrated Logging and Monitoring with option to create alerts based on performance anomaly based on Machine Learning.	
11	Service version Upgrade with customer having control over the Upgrade window.	
12	Automated Operating System Patching with customer having control over the Patching window.	

13	CSP should offer the facility to support Active-Active/Active-Passive architecture having Business continuity plan with built in fault tolerance to avoid any failure at the underlying hardware infrastructure.	

Web Application Firewall

S No	Eligibility Criteria	Compliance(Y/N
1	Cloud platform should provide Web Application Filter for OWASP (Open Web Application Security Project) Top 10 protection	
2	Service provider WAF should be able to support multiple website security.	
3	Service provider WAF should be able to perform packet inspection on every request covering all layer 7.	
4	Service provider WAF should be able to block invalidated requests.	
5	Service provider WAF should be able to block attacks before it is posted to a website.	
6	Service provider WAF should have manual control over IP/Subnet. i.e., Allow or Deny IP/Subnet from accessing websites.	
7	The attackers should receive custom responses once they are blocked.	
8	Service providers must offer provision to customize responses to vulnerable requests.	
9	Service provider WAF should be able to monitor attack incidents and simultaneously control the attacker IP.	
10	Service provider WAF should be able to Whitelist or Blacklist IP/Subnet.	
11	Service provider WAF should be able to set a limit to maximum number of simultaneous requests to the web server and should drop requests if the number of requests exceed the threshold limit.	
12	The WAF should be able to set a limit to the maximum number of simultaneous connections per IP. And should ban / block the IP if the threshold is violated.	
13	WAF should be able to set a limit to maximum file size, combined file size in bytes	
14	WAF should be able to limit allowed HTTP versions, request content type, restricted extensions and headers	
15	Service provider WAF should be able to limit the maximum number of arguments, argument name, value, value total length etc.	

CSP Native SIEM Solution

S No	Eligibility Criteria	Compliance(Y/N
1	The platform must provide a fully managed Cloud-native SaaS solution from the CSP without any dependency on third parties that requires no maintenance or core monitoring, with systems and security maintained 24x7.	
2	The platform must offer a seamlessly integrated, advanced SOAR, complete with playbook testing, playbook health monitoring, a comprehensive Integrated Development Environment (IDE), and a diverse marketplace for integrations.	
3	The platform must include a built-in, integrated User and Entity Behavior Analytics (UEBA) functionality and capability within its SaaS instance of the platform, supporting 3rd party data log sources from various vendors.	
4	The platform must support a single integrated SIEM/SOAR/UEBA functionalities within a single SaaS application and a single pane of glass.	
5	"The platform must automatically enrich events at data ingestion to enable rapid lookup across multiple large sets of data over a 12-month old data to achieve: 1) More Simple& Readable Rules and Search Queries 2) Enrichment context which is dynamic & correct with respect to time frame 3) Reduction in table joins / performance demands 4) Ability to perform historical enrichment for data over 12 months (i.e user-IP mapping, Geolocation info)"	

6	The platform must provide embedded hot storage by default for 12 months to cater for extended retroactive search and forensic investigations at no additional cost.	
7	The platform must have the SIEM/SOAR services delivered specifically in-country as a region, as confirmed by publicly available documents.	
8	The solution must be a cloud-native SaaS application leveraging core Cloud Service Provider (CSP) services in order to ensure maximum resiliency.	
9	The platform must have a dedicated cloud-native SaaS infrastructure in the country. Core services for both Data at Rest and Data in Transit should be within the country region. If any services are run outside of a country, adequate security mechanisms must be in place to safeguard against unauthorized access, tampering, and modifications.	
10	The Platform must have Incident Management capabilities for coordination during high impact incidents.	
11	The platform must have the capability to facilitate collaboration with end users external to the operating organization, enabling them to approve elements of playbook automation and case management.	
12	The Platform's playbook building must be based on a drag and drop approach with no coding required and includes a Playbook Simulator to test playbooks against production or sample data for validation.	
13	The Platform must support creation of bespoke alert views on each playbook for specific SOC roles, ensuring that each SOC role user will see information specific to their needs when performing the investigation.	
14	The platform must have the capability to support integrating third party intelligence feed	
15	The solution should come with out-of-the box detection rules covering on-prem and cloud threats.	

4. Pre-Qualifications (PQ) Criteria:

The CSP must be empaneled with the Ministry of Electronics and Information Technology(MeitY) and should be STQC Audited.
The bidder must comply with each of the below listed PQ eligibility criteria to qualify for the technical qualification.

4.1 Criteria for CSP (Cloud Service Provider)

Sr.No	BasicRequirement	Eligibility Criteria	Document to be submitted
1	Legal Entity	The CSP should be a Legal Entity registered under the Companies Act, 2013 or the Companies Act, 1956 OR a Limited Liability Partnership (LLP) registered under the LLP Act, 2008 or Indian Partnership Act 1932.	Copy of Certificate of Incorporation/Registration/Partnership deed
2	MeitY Empanelment	The CSP should be MeitY empaneled (as on bid submission date). The proposed Data Centre should be within India. The proposed Data Centre should be successfully STQC audited.	Valid copies of proof attested by authorized Bid signatory
3	Compliance	The CSP is compliant with IT Act 2000 (including 43A) and amendments	Letter from authorized signatory on the letter head of bidder mentioning the compliance.
4	Turnover	The CSP should have an average turnover of at least 1000 Crore in last three audited financial years from cloud services (FY 2021- 2022, 2022-2023 and 2023-2024).	Certificate from the Statutory Auditor/Chartered Accountant
5	Net worth	The CSP should have positive net worth as per last audited financial report.	Certificate from the Statutory Auditor/Chartered Accountant
6	Blacklisting	The CSP should not be debarred/ blacklisted by any Government/PSU in India as on date of submission of the Bid.	Letter signed by the Authorized in format given in the RFP.
7	Data Centre Facility	The Data Centre should be at least Tier III standard (certified under TIA 942 or Uptime Institute certifications) and implement tool- based processes based on ITIL standards.	Valid copy of the certificate
8	Data Center Certification	Certification: ISO 27001 – Data Centre and the cloud services should be certified for the latest version of the standards. ISO/IEC 27017:2015-Code of practice for information security controls based on ISO/IEC 27002 for cloud services and Information technology. ISO 27018 – Code of practice for protection of personally identifiable information (PII) in public clouds. ISO/IEC 42001:2023 Compliance. ISO-22301 for Business Continuity Management. ISO/IEC 20000-9-Guidance on the application of ISO/IEC 20000-1 to cloud services. PCI DSS – compliant infrastructure for storing, processing, and transmitting credit	Valid copy of the certificate/CSP Undertaking

		card information in the cloud.	
9	DC – DR Configuration	The CSP must be operating in multiple Data Centres in India. DC-DR should not be in the same data center. Note:- DC and the DR should be in different seismic zones.	Letter from Authorized signatory on the letter head of the bidder..
10	DR Site	The proposed DR site should be decided based on the risk assessment to confirm that the DR location does not share the same risks of the department primary Data Centre. Note:- The secondary Data Center shall be located in a different seismic zone and at least 100 Kms away from the primary Data Centre.	Letter from Authorized signatory on the letter head of the bidder.
11	Experience	The CSP should have successfully implemented / commissioned at least Ten (10) projects of DC/DR with Cloud services provided on MEITY (Ministry of Electronics and Information technology) empaneled cloud for any central/state Govt/PSU or government body/ institution in India during last five financial years (2019-20, 2020-21, 2021-22, 2022-23, 2023-24) and till the date of Bid submission.)	Work order/contract + completion certificate from client/undertaking of work in progress from bidder
12	Advance Security	The CSP should have accreditations relevant to security, availability, confidentiality, processing integrity, and/or privacy Trust Services principles. SOC 1, SOC 2, SOC 3	Valid copy of the certificate
13	Tax Payment	The CSP must have a valid GST Registration in India and PAN	Valid copy of the certificate
14	Capability	The CSP should provide the department the flexibility to create resources like Virtual instance, storage and other services of custom configuration such as 6 vCPU and 16 GB RAM, 20 vCPUs and 40 GB RAM etc. and should not restrict to specific configuration.	Letter from Authorized signatory on the letter head of the bidder.
15	Public Pricing	The proposed cloud should have public price in INR on the Public calculator for the price validation and verification	Public Links and Letter from Authorized signatory on the letter head of the bidder.
16	GPU	The CSP must have GPU based machines as one of the publicly listed services. The minimum Technical Specifications of GPus: FP64 - 34 teraFLOPS FP32 - 67 teraFLOPS GPU Memory- 80GB	Public Links and Letter from Authorized signatory on the letter head of the bidder.

17	Cloud AI/ML	The CSP should have native Unified End-to-End AI/ML Platform as Managed Service : • Managed services for Model training • Build, orchestrate, and automate reproducible ML workflows, easing the transition from experimentation to production • Centralized repository for managing, versioning, and tracking trained ML models • Flexible model serving options (online or batch prediction) at scale with optimized infrastructure • Manage and deploy multiple models or model versions behind a single API endpoint for simplified model serving	Public Links and Letter from Authorized signatory on the letter head of the bidder.
18	Cloud Security	The Proposed CSP should have native SIEM platform that drive consistency in response and automate the repetitive tasks to protect the organization against modern-day threats with following features: 1) Unified experience in detection, investigation, and response by collecting security telemetry data to identify high priority threats, drive response. 2) Raw log message in original format along with the enriched data for 1 year as hot storage with local instance for data sovereignty. 3) Ability to check indicators of compromise against 12 months' worth of history automatically upon ingestion of a new IOC retroactively.	Public Links and Letter from Authorized signatory on the letter head of the bidder.
	Cloud Security	Centralized Security solution providing a single, consolidated view of the organization security posture covering the following features: • Proactive and Reactive • Vulnerability Scanning • Threat Detection • Compliance Monitoring • Risk Prioritization • Incident Response • Discovery and Inventory	Public Links and Letter from Authorized signatory on the letter head of the bidder.
19	Cloud Native Database	The proposed Cloud should have CSP Native Managed database services for MS-SQL EE and Std. , PostgreSQL and My-SQL with Monthly Uptime Percentage SLA of 99.99%	Public Links and Letter from Authorized signatory on the letter head of the bidder.
20	Cloud Native CDN	The proposed Cloud should have the CSP Native CDN service with Compliances mentioned for CDN in Annexure in the RFP	Public Links and Letter from Authorized signatory on the letter head of the bidder.

Cloud Native CDN (Content Delivery Network) compliances

Sr. No	Service Requirements Specification	Description	Document to be submitted
1	On-Demand Scalability	Delivery of live streaming with websites/ on-demand/ Archived Videos/ Audio/ Podcasting Services by improving the end user experience via peak load handling & high availability. The CDN services shall be able to scale incrementally to meet demand during the event or at the time of content delivery/distribution	Public Links or Letter from Authorized signatory on the letterhead
2	Geographical Locations	Geographical locations across India	Public Links or Letter from Authorized signatory on the letterhead

3	Reliability	The CDN Service Provider shall ensure that the proposed services shall be available 99.9% of the time.	Public Links or Letter from Authorized signatory on the letterhead
4	Performance	The content delivered through the CDN services shall not degrade the performance of the origin website or content in any manner, even if the number of hits on the website increases exponentially. The CDN Service Provider should have adequate / spare capacity available to handle spikes in traffic.	Public Links or Letter from Authorized signatory on the letterhead
5	Supported Device	The CDN service shall support all types of desktop and mobile devices	Public Links or Letter from Authorized signatory on the letterhead
6	Traffic Handling Capacity/Bandwidth	More than 10 GBPS	Public Links or Letter from Authorized signatory on the letterhead
7	Points of Presence in India	Minimum 3 PoPs	Public Links or Letter from Authorized signatory on the letterhead
8	Geo Fencing/Geo Restriction	Yes	Public Links or Letter from Authorized signatory on the letterhead
9	Protection of CDN against volumetric attack on Network Layer 3,4,7 etc.	TCP state exhaustion attacks, HTTP and UDP flood attacks, Reflective amplification attacks etc.	Public Links or Letter from Authorized signatory on the letterhead
10	TLS/SSL (Per Certificate)	Any	Public Links or Letter from Authorized signatory on the letterhead
11	Real time monitoring of reporting	The view should be customizable with minimum 5 role-based and management features access for each website separately. There should not be any restrictions on the number of users and concurrent logins.	Public Links or Letter from Authorized signatory on the letterhead
12	Monthly uptime	99.90%	Public Links or Letter from Authorized signatory on the letterhead
13	Change request for any addition / removal of website should be implemented	Within 48 Hours	Public Links or Letter from Authorized signatory on the letterhead
14	Self-Provisioning	CDN should have self-provisioning interface to configure, monitor and manage the cached data and its life cycle	Public Links or Letter from Authorized signatory on the letterhead
15	Cache content Availability	99.50%	Public Links or Letter from Authorized signatory on the letterhead
16	The http/https calls to origin server should be minimized log delivery	Web Application Firewall deployment should be POP to achieve high scalability and availability	Public Links or Letter from Authorized signatory on the letterhead
17	Change/Update TLS	CDN Owner / Channel Partner would be responsible to update latest certificates	Public Links or Letter from Authorized signatory on the letterhead
18	Whitelisting of IPs	Whitelisting of edge IPs/ range IP of IPs preferable in India	Public Links or Letter from Authorized signatory on the letterhead
19	Security of Data	Security of data' also encompasses integrity and confidentiality during transit. Data should not be leaked to a third party prior to publishing	Public Links or Letter from Authorized signatory on the letterhead
20	Should be capable for handling HTTPS 2 and HTTPS3	The communication between origin and edge servers should also be on HTTPS	Public Links or Letter from Authorized signatory on the letterhead
21	Number of websites and live streams	There should not be any restriction in number of websites and number of livestreams	Public Links or Letter from Authorized signatory on the letterhead
22	Points of Presence Globally	Minimum 50 PoPs	Public Links or Letter from Authorized signatory on the letterhead

4.2 Criteria for MSP (Managed Cloud Service Provider) (Bidder)

#	Basic Requirement	Eligibility Criteria	Document to be submitted
1	Legal Entity	The MSP should be a Legal Entity registered under the Companies Act, 2013 or the Companies Act, 1956 and in operation for at least 10 years as on 31.03.2024. Consortium or JV not allowed	Copy of Certificate of Incorporation/Registration/Partnership deed
2	Office	The MSP must have a local office in India	Copy of address proof
3	Compliance	The MSP is compliant with IT Act 2000 (including 43A) and amendments	Letter from authorized signatory on the letter head of bidder mentioning the compliance.
4	Turnover	The MSP should have average annual turnover of at least 150 Crore from IT/ITeS in last three audited financial years (FY 2021-2022, FY 2022-2023 & FY 2023-2024).	Certificate from the Statutory Auditor/Chartered Accountant
5	Net worth	The MSP must have a positive Net Worth in each of the three FY i.e. FY 21-22, FY 22-23 & FY 23-24 as per last audited financial report.	Certificate from the Statutory Auditor/Chartered Accountant
6	Blacklisting	The MSP should not be debarred/ blacklisted by any Government/PSU in India as on date of submission of the Bid.	Letter signed by the Authorized in format given in the RFP.
7	Legal	The bidder should not be subjected to any legal action for any cause in any legal jurisdiction in the last five years.	Letter signed by the Authorized
8	Experience - 1	Bidder should have successfully implemented / commissioned at least One (01) projects with MeitY empaneled CSPs DC and DR with Cloud Deployment for any state / central government entities.within the last five years i.e. FY 2019 - 2024 in India . The project should have a minimum project value of INR 30 crore (Only cloud component value will be considered – clear bifurcation and client certificate should be provided for value of the project). The projects must include: 1. Management and provisioning of Cloud Services on	Work order + completion certificate from client

		Meity Empaneled Cloud. 2 Achieved go-live/operational acceptance. 3. Operated for a period of at least one year.	
10	Experience - 2	The Bidder should have similar experience of Cloud services in India during last 5 years as on date of submission of bid. The Bidder should have executed similar project experience/Work order as follows: Note: 1) Similar work means managed services for cloud infrastructure on MeitY (Ministry of Electronics and Information technology) empaneled cloud for Central Govt / State Govt in India. Such similar works should cover minimum infrastructure as below in a single project, as on the date of submission of the bid: · 5000 vCPU · Enterprise Networking Solution · Enterprise Security Solution ·1000 TB storage · Enterprise grade firewall · Data Migration from on premises server to cloud (MeiTY empaneled CSP) of over 500TB. 2) For the above experience, **only go-live projects shall be considered** 3) Further ongoing projects, will be considered if Go-live declared on or before date of bid publishing. In case of ongoing projects, the value of similar works completed will be considered for evaluation.	Work order + completion certificate from client
11	Certification	Following ISO and CMM Certifications certifications as on Bid submission Date: 1. ISO 9001 2. ISO 27001 3. ISO 20000-1 4. ISO 22301 5. ISO 27017 6. ISO 27018 7. CMMi5	Valid Copy of the Certificate to be attached.
12	Manpower Strength	The Bidder must have strength of at least 200 IT Professionals (Data Centre / networking / system administration / cloud services professional's / cloud security experts etc.) on their payroll as on date of submission of this bid. The bidder should have minimum 20 certified cloud resources out of the above mentioned 200 resources on the proposed cloud platform on their payroll These certified cloud resources should be on Bidder's payroll for 6 months or more as on bid submission date.	Certificate from HR on the letter head of the bidder certifying the availability of the resources on their payroll as on date of submission of the bid as per the requirement along with valid CSP certification copy

13	Tax Payment	The MSP must have a valid GST Registration in India and PAN	Valid copy of the certificate
14	Capability	The MSP should provide department the flexibility to create resources like Virtual instance, storage and other services of any configuration and should not restrict to specific configuration.	Letter from Authorized signatory on the letter head of the bidder.
15	Billing	The bidder should have Direct billing relationship with Proposed CSP	Confirmation letter on the letter head of the MSP or Agreement executed with proposed CSP & MSP.
16	Authorization	Bidder to provide MSP authorization letter from the MeitY Empaneled CSP quoting this tender reference number, date, and due date of opening along with the bid	MSP Authorization Certificate to MSP with empanelment confirmation of CSP

5. Technical Evaluation and Marking Criteria

5.1 Technical Qualification

The technical Bids along with all the supporting documents shall be submitted in separate folder. Department will review the technical bids of the MSP to determine whether the technical bids are substantially responsive. Bids that are not substantially responsive are liable to be disqualified at department's discretion. The MSP's technical solutions proposed in the bid document will be evaluated as per the requirements specified in the RFP and technical evaluation framework. The Bidder would be required to cover the following but not limited to:

- Overall Cloud architecture including solution design
- Project Management and Implementation Methodology
- Migration Plan
- Integration approach with other IT Infrastructure
- Maintenance and Support for proposed solution
- Risk Mitigation plan
- Each Technical Bid will be assigned a technical score out of a maximum of 100 marks.
- Only the bidders who obtain an overall cut-off technical score of 70% will qualify for the commercial evaluation stage.

Failing to secure minimum marks shall lead to technical rejection of the Bid and Bidder.

5.2 Technical Evaluation criteria

Criteria for CSP and MSP (Managed Cloud Service Provider)

Sr.No	Evaluation Criteria	Criteria	Marks (Max)
1	The proposed cloud data lake platform should have End-to-end ML using SQL applications building on the same platform to save the deployment cycle, effort and cost with SLA of 99.99% to enhances the reliability and user experience	URL of the service on the CSP through Self provisioning portal	2
2	The proposed Cloud should have Native security services- 1) WAF & DDoS Protection with enterprise features such as Threat Intelligence, Third-party named IP address & Adaptive Protection 2) Threat detection, Vulnerability Assessment, Bot management with captcha Integration 3) Cloud Native Security services for both - IDS and IPS and Cloud-native SaaS SIEM solution from the CSP without any dependency on third party 4) Continuous virtual red teaming including attack paths, risk scoring, and toxic combinations, 5) Cloud security and risk management for multi-cloud environments 6) Security posture management, attack paths, threat detection, and compliance monitoring Subscription-based pricing for multi-cloud	URL of the service on the CSP through Self provisioning portal	2
3	The proposed Cloud should have Native Storage service for different IOPS, and should have capability to increase storage capacity on demand on the provisioned volumes without any reboot of the virtual machine. The volume should be Regional redundant to zero down the impact of single AZs failure & support 64 TB per volume with Sub-millisecond latency performance.	URL of the service on the CSP through Self provisioning portal	2
4	The CSP should have following services with SLA of : - Ease of custom configurations of VM's for self- provisioning based on the Custom vCPU and RAM - Single Instance SLA : >= 99.9% and Instances in Multiple Zones : >= 99.99% - PBs scale Serverless Data Lake Service with SLA of >= 99.99% and capabilities of GenAI Integration and inbuilt Machine learning models	URL of the service on the CSP Self provisioning portal	2

5	CSP or parent company provided native state-of-the-art its own multi-modal LLM model for Text Generation, Summarization, Chatbots and Conversational deployed on the CSP native fully managed AI Platform and to be demonstrated : 1. CSP provides its own multi model - 7 marks 2. CSP provides open source /3rd party/ (not own by CSP) - 5 marks	URL of the service on the CSP through Self provisioning portal or Demonstrate during the Presentation	7
6	The proposed Cloud should have Managed cloud native enterprise database services for MySQL and PostgreSQL with the following features: 1) Enterprise Database services with 99.99% SLA 2) Automated backups and point-in-time recovery 3) Automatic Storage Increase 4) Automated replication/Automatic failover to another Zone 5) Multi -AZs HA architecture with Sync replication	URL of the service on the CSP through Self provisioning portal	10
7	"The CSP should have native Unified End-to-End AI/ML Platform as Managed service that focus on MLOps&LLMOps principles which includes: 1. Managed services for Model training 2. Build, orchestrate, and automate reproducible ML workflows, easing the transition from experimentation to production 3. Centralized repository for managing, versioning, and tracking trained ML models 4. Flexible model serving options (online or batch prediction) at scale with optimized infrastructure 5. Manage and deploy multiple models or model versions behind a single API endpoint for simplified model serving 6. Platform must provide flexibility to deploy model on a private endpoint and also to be able to export a model to make it portable, like running in a container" 7. Language translation service in speech to speech, speech to text, text to speech and text to text for Indian languages.	URL of the service on the CSP through Self provisioning portal	5
8	The proposed Cloud Should have Managed cloud native Kubernetes service with the following features: 1) Binary Authorization Secure Verified Container Images for software supply-chain security 2) Container Threat Detection as inbuilt service with Dashboard 3) Vertical Pod Autoscaler and Node auto-upgrades 4) Native Kubernetes backup & restore service	URL of the service on the CSP through Self provisioning portal	5
9	CSP Native Enterprise Grade API Management turnkey solution (* Not API Gateway) for publishing APIs to external and internal consumers through an integrated out of the box developer portal, Monetization, Advanced API Security like Bot Detection and API configuration security scoring, and should be able to deploy as a SaaS cloud offering and multi-clouds deployment option for the data plane	URL of the service on the CSP through Self provisioning portal	5

10	The MSP must have the any of 4 following ISO and CMM Certifications certifications as on Bid submission Date: 1. ISO 9001 2. ISO 27001 3. ISO 20000-1 4. ISO 22301 5. ISO 27017 6. ISO 27018 7. CMMi5 Mandatory Requirement: The CMMi Certificate must be validated on https://cmmiinstitute.com website. Failure to which the bidder will be disqualified during the bid evaluation stage.	4 Certificates: 4 Marks 5 Certificates: 6 marks 6 Certificates : 8 marks 7 Certificates: 10 marks	10
11	The Bidder should have similar experience of Cloud services in India during the last 5 years of date of submission of bid. The Bidder should have executed similarcloudproject experience/Work order as follows: Note: 1) Similar work means managed services for cloud infrastructure on MeitY (Ministry of Electronics and Information technology) empaneled cloud for Central Govt / State Govt in India. Such similar works should cover minimum infrastructure as below, as on the date of submission of the bid: · 5000 vCPU · Enterprise Networking Solution · Enterprise Security Solution · 1000 TB storage · Enterprise grade firewall · Data Migration from on premises server to cloud of over 500TB. 2) For the above experience, only completed projects shall be considered. 3) Further ongoing projects will be considered if Go-live is declared on or before the date of bid publishing. In case of ongoing projects, the value of similar works completed will be considered for evaluation.	No of vCPU(s) 5000 to 6000 - 4 Marks 6001 to 7000 - 6 Marks More than 7001 - 8 Marks Storage 1000 TB to 1000 TB - 4 Marks 1101 TB to 1200 TB - 6 Marks More than 1200 TB - 8 Marks Data Migration from on premises server to cloud (MeiTy empaneled CSP) 500TB to 1000 TB - 2 Marks Above 1000 TB - 4 Marks	20
12	**Technical Demonstration (Use Case*) Marks are indicated against each use case.**	**The bidder shall be required to give a technical demonstration of the proposed cloud platform. For this purpose, the Bidder's proposed resource personnel shall demonstrate the use cases* as listed, during the scheduled Demonstration. The date & time for the demonstration shall be communicated later.**	

1	CSP SSD Storage Tiers with IOPS (as per BoQ), Throughput, High availability for DC to DR replication: 1. Configure SSD Storage with specific IOPS/Throughput and attach to the VM in Specific Region 2. Configure SSD Storage volume in Multi-AZs/redundant architecture to avoid single AZ failure 3. Configure Storage volumes replication from DC to DR for near zero RPO or < 5 mins of RPO as per RFP 4. Ingest dummy records in the DC VM and shows the logs/Dashboards that shows the data movement to DR side disk/VMs 5. Demonstration of the ingested records (full records ingested in the DC) in the DR VM 6. Object Storage data lifecycle policy, ingest data in Archive Storage and Restore Archived data in sub-millisecond 7. Creation and Demonstration of the Object Storage buckets with DC to DR replication configuration CSP native SIEM platform that drives consistency in response and automates repetitive tasks to protect the organization against modern-day threats with following features. The Bidder should show the CSP native SIEM Platform with listed capabilities through the presentation and submit the deck to committee for Reference: 8) Unified experience in detection, investigation, and response by collecting security telemetry data to identify high priority threats, drive response. 9) The solution should come with out-of-the box detection rules covering on-prem and cloud threats. 10) The Platform's playbook building must be based on a drag and drop approach with no coding required and includes a Playbook Simulator to test playbooks against production or sample data for validation. 11) The Platform must have Incident Management capabilities for coordination during high impact incidents.	7 - 8 : 10 marks > 9 : 15 marks	15
2	Details Presentation of the Proposed Solution , Proposed Security ,Detailed approach & methodology for providing technical support to the project and escalation matrix - to be done by MSP		15
		Total Marks	**100**
Qualifying Marks			**70**

Evaluation shall be done based on the information provided in the technical proposal (and subsequent clarification, if any) and Clarifications / Answers given by the bidders to department during the Presentation and Site visit.

Only the bidders who obtain an overall cut-off technical score of 70% will qualify for the commercial evaluation stage. Failing to secure minimum marks shall lead to technical rejection of the Bid and Bidder.

The evaluation will be done based on the parameters given below:

The bidders who clear the pre-Qualification criteria as per Section 4.1 will be considered for technical evaluation.

Financial bid will be opened on GeM.

Technical evaluation will be done based on the below calculations.

Formula.

$$\frac{\text{Total marks of the respective vendor}}{\text{Total Technical Marks (100 Marks)}} \times 100$$

$$\text{MSP 1} = \frac{\text{Technical Score Marks x Technical Weightage i.e., 70\% 70 Marks}}{\text{100 Marks}} \times 100 = 70 \qquad 70 \times 0.7 = 49$$

Bidder	Combined Marks (A)	Out of (B)	Tech Marks (TM)= A/B*100	Tech. Weightage TW = 0.7	Tech. Marks TMW = TM x TW
MSP 1	70	100	70	0.7	49
MSP 2	75	100	75	0.7	52.5
MSP 3	68	100	68	0.7	47.6

5.3 Technical Proposal

As part of the Technical Proposal, Bidder must fulfil the Pre-qualification criteria and submit the same along with Indicative Technical Bill of Material in section 5.4 with MSP Published prices against each line item.

5.4 Indicative Technical Bill of Material

The Bidders must submit the indicative technical bill of material along with technical bid

Indicative Technical Bill of Material

S.No.	Service Name / Type of Service	Configuration/Description of Service	Specifications of required Service	Unit of Measurement of Service	Proposed	Total Indicative Hours in a Month / Billing Cycle
A. Compute as Managed Service						
1	Non burstable x86 architecture - Production Grade Virtual Machine - on demand	RED HAT Enterprise Linux Including cloud Licenses and native billing for RHEL	VM - 2 vCPU, 4GB RAM	Monthly	1	730
2			VM - 2 vCPU, 8GB RAM	Monthly	1	730
3			VM - 2 vCPU, 16GB RAM	Monthly	1	730
4			VM - 4 vCPU, 8GB RAM	Monthly	2	730
5			VM - 4 vCPU, 16GB RAM	Monthly	5	730
6			VM - 4 vCPU, 32GB RAM	Monthly	3	730
7			VM - 8 vCPU, 32GB RAM	Monthly	2	730
8			VM - 16 vCPU, 64GB RAM	Monthly	2	730
9			VM - 32 vCPU, 128GB RAM	Monthly	4	730
10			VM - 48 vCPU, 192GB RAM	Monthly	2	730
11			VM - 64 vCPU, 256 GB RAM	Monthly	1	730
12			VM - 80 vCPU, 320 GB RAM	Monthly	1	730
13			VM - 96 vCPU, 384 GB RAM	Monthly	1	730
14			VM - 128 vCPU, 512 GB RAM	Monthly	1	730
15			VM - 224 vCPU, 224 GB RAM	Monthly	1	730
16		Open-Source Linux - Debian, CentOS, Ubuntu	VM - 2 vCPU, 4GB RAM	Monthly	30	730
17			VM - 2 vCPU, 8GB RAM	Monthly	25	730
18			VM - 2 vCPU, 16GB RAM	Monthly	20	730
19			VM - 4 vCPU, 8GB RAM	Monthly	40	730
20			VM - 4 vCPU, 16GB RAM	Monthly	150	730
21			VM - 4 vCPU, 32GB RAM	Monthly	5	730
22			VM - 8 vCPU, 32GB RAM	Monthly	75	730
23			VM - 16 vCPU, 64GB RAM	Monthly	40	730
24			VM - 32 vCPU, 128GB RAM	Monthly	50	730
25			VM - 48 vCPU, 192GB RAM	Monthly	10	730
26			VM - 64 vCPU, 256 GB RAM	Monthly	30	730
27			VM - 80 vCPU, 320 GB RAM	Monthly	10	730
28			VM - 96 vCPU, 384 GB RAM	Monthly	10	730
29			VM - 128 vCPU, 512 GB RAM	Monthly	40	730
30			VM - 224 vCPU, 224 GB RAM	Monthly	20	730
31		Windows O/S with Cloud Based O/S Licenses & native billing	VM - 2 vCPU, 8GB RAM	Monthly	25	730
32			VM - 4 vCPU, 16GB RAM	Monthly	135	730
33			VM - 8 vCPU, 32GB RAM	Monthly	200	730
34			VM - 16 vCPU, 64GB RAM	Monthly	30	730
35			VM - 32 vCPU, 128GB RAM	Monthly	5	730
36			VM - 48 vCPU, 192GB RAM	Monthly	5	730
37			VM - 64 vCPU, 256 GB RAM	Monthly	5	730
38			VM - 80 vCPU, 320 GB RAM	Monthly	5	730
39			VM - 96 vCPU, 384 GB RAM	Monthly	5	730

40			VM - 128 vCPU, 512 GB RAM	Monthly	10	730
B. Storage as a Managed Service - Object, File and Block Storage						
1	Object Storage - Hot Tier	Managed Object Storage	Fully Managed Redundant Object Storage - 100% Hot Tier	TB per month	1200	Monthly
2	Archive Storage with milliseconds restore tier	Managed Archival Storage - Restored quickly in milliseconds	Fully Managed Geo Redundant Archival/ Cold Tier with instant restore time	TB per month	1500	Monthly
3	Cloud Native Enterprise-grade network file system (NFS)	Enterprise-grade network file system (NFS)	TB of provisioned capacity	TB Per Month	30	Monthly
4	Managed Storage- SSD	Managed SSD Storage for Mission Critical Web, Apps and Databases	Single SSD redundant volume with 6,000 Provisioned IOPS/TB or 6 IOPS /GB from Storage tier which support 64 TB per volume with Sub-millisecond latency performance.	TB per month	500	Monthly
5			Single SSD redundant volume with 30,000 Provisioned IOPS/TB or 30 IOPS /GB from Storage tier which support 64 TB per volume with Sub-millisecond latency performance.	TB per month	600	Monthly
C. Managed DB - Native Managed services by CSP						
1	CSP Native Managed Database services (Non burstable x86 Intel architecture - Production Grade)	PostgreSQL /MySQL as a service with following features: 1) Automated backups and point-in-time recovery 2) Automatic Storage Increase 3) Support Multi AZ architecture with Sync Replication 4) Should	2 vCPU 8 GB RAM	Monthly	1	730
2			4 vCPU 16 GB RAM	Monthly	1	730
3			8 vCPU 32 GB RAM	Monthly	1	730
4			16 vCPU 64 GB RAM	Monthly	1	730
5			32 vCPU 128 GB RAM	Monthly	1	730
6			48 vCPU 192 GB RAM	Monthly	1	730
7			64 vCPU 256 GB RAM	Monthly	1	730
8			96 vCPU 384 GB RAM	Monthly	1	730

		support horizontal scaling by adding/removing read replicas Bidder must Quote the CSP Managed DB Service with HA architecture & Configuration (e.g. Active/Standby) for the Pricing				
9		MS SQL Server 2017 / 2019 / 2022 Enterprise as a service with following features: 1) Automated backups and point-in-time recovery 2) Automatic Storage Increase 3) Support Multi AZ architecture with Sync Replication 4) Should support horizontal scaling by adding/removing read replicas Bidder must Quote the CSP Managed DB Service with HA	2 vCPU 8 GB RAM	Monthly	1	730
10			4 vCPU 16 GB RAM	Monthly	1	730
11			8 vCPU 32 GB RAM	Monthly	1	730
12			16 vCPU 64 GB RAM	Monthly	1	730
13			32 vCPU 128 GB RAM	Monthly	1	730
14			48 vCPU 192 GB RAM	Monthly	1	730
15			64 vCPU 256 GB RAM	Monthly	1	730
16			96 vCPU 384 GB RAM	Monthly	1	730

		architecture & Configuration (e.g. Active/Stand by) for the Pricing				
17		MS SQL Server 2017 / 2019 / 2022 Standard as a service with following features: 1) Automated backups and point-in-time recovery 2) Automatic Storage Increase 3) Support Multi AZ architecture with Sync Replication 4) Should support horizontal scaling by adding/removing read replicas Bidder must Quote the CSP Managed DB Service with HA architecture & Configuration (e.g. Active/Stand by) for the Pricing	2 vCPU 8 GB RAM	Monthly	1	730
						730
						730
18			4 vCPU 16 GB RAM	Monthly	1	730
19			8 vCPU 32 GB RAM	Monthly	1	730
20			16 vCPU 64 GB RAM	Monthly	1	730
21			32 vCPU 96 GB RAM	Monthly	1	730
22			48 vCPU 128 GB RAM	Monthly	1	730
23	CSP Native Redis Cluster as Service - Production Grade	Managed Redis as a Service with: - Should support the Managed	130 GB Enterprise Grade Redis with Sharding support	Monthly	15	730

	supporting Sharding	Cache database service - Supports partitions/shards and read replicas - Must be compatible with open-source Redis data store - Inbuilt capability to auto-scale shards and read replicas - Persists data stored in Redis Cache - Shards data across Redis nodes				
24	Production Grade CSP Native Managed Non-Relational Database(NoSQL) as Managed Services	Scalable NoSQL DB as Managed Service 1) Automated replication/Automatic failover to another Zone and region 2) Automated Backup 3) Multi -AZs HA architecture	Storage (GB) - 500 , Number of writes / Second: 1000 , Number of reads / Second: 2000, Backup - 30 days	Monthly	15	730
D: Other CSP Managed /additional services/Network /Back up / Security						
1	CSP native Container Registry	Container Registry allows you to build, store, and manage container images and artifacts in a private registry for all types of container	Container Registry - 100GB/Month	100GB/ Month	2	Monthly

2	Managed Kubernetes (Production Grade, SLA Backed)	Container Orchestration service to deploy, scale and manage container-based applications in a cluster environment. Should support service mesh for observability, network and security.	Fully Automated highly available & scalable managed Kubernetes Cluster / Month	Monthly	2	730
3	Cloud Management and Monitoring	Monitoring, Logging & Alerts for cloud resources	Monitoring and observability service, with data and actionable insights to monitor applications, respond to system-wide performance changes, optimize resource utilization, and a unified view of operational health.	Logs of 1000 GB per month.	1	Monthly
4	Site to Site VPN - CSP Managed Service	Fully managed Site to Site VPN	VPN Connectivity as Site-to-Site VPN with upto 1.25 Gbps bandwidth per VPN tunnel	Monthly	50	Monthly
5	DevOps and Application Monitoring	CI/CD Pipeline (Should provide a fully managed build service that supports continuous integration and deployment.)	Continuous Integration and Code Deployment Pipelines with min 5 users	Per month	10	Monthly
6			Build Minutes [Min 4 vCPU and 8GB RAM build server]	100hrs/Per month	10	Monthly
7	CSP Natively Managed Application Load balancer (L7)	Managed service to provide automated traffic distribution from one entry point to multiple back ends over layer 7	Should provide an Application Gateway as an external facing layer 7 load balancer which supports SSL termination, cookie-based session affinity and round robin for load-balancing traffic. Load Balancers with data being processed up to 1TB/month	Per month	20	Monthly
Added	SSL Certificate				200	Monthly

8	CSP Natively Managed TCP Load balancer(L3/ L4)	Managed service to handle high volumes of TCP traffic	Load Balancers with data being processed up to 1TB/month	Per month	50	Monthly
9	NAT Gateway	Managed NAT Gateway for outbound Internet Access for Private Instances	100GB of data Processed/Month	Per month	10	Monthly
10	Backup as Service	Full managed backup service	Back up key data stores, such as volumes, databases, and file systems, across cloud resources, Policy based Centralize & automated data protection management and Backup role-based access control , Backup activity monitoring	per TB / per month	50	Monthly
11	Domain Name System (DNS)	Managed DNS service that supports all common DNS record types with following features: - Weighted round robin (WRR) routing policy - Geofenced routing policy - Failover routing policy	Per Domain Name per month	With 5 Hosted Zone and 50 Million Queries	10	Monthly
12	Data transfer /Egress over the Internet	Data Transfer Egress from Compute , database, Object Storage etc. over the Internet	Data transfer out per month	Per GB	10000	Monthly
13	Direct Connect / Interconnect to connect	Interconnect Port with capacity of 1 Gbps	Link termination inside a VPC	Per Port	1	

	MPLS/ Lease Line to cloud					
14	Messaging services	Should provide a managed message queueing service for communicating between decoupled application components	Standard queue requests and FIFO queue requests in millions /1GB Volume with number of Subscriptions per Month	Monthly	1	Monthly
15	Public IP	Public IP for VMs and LBs	Per Public IP	Monthly	150	Monthly
16	CSP Native SIEM Enterprise solution	Raw log information for building detection capability, improving risk analytics, and extending logs for investigating .	Ingestion in GB	Monthly Per GB	2500	Monthly
17	Cloud Posture Management	Identify cloud misconfigurations, software vulnerabilities, and compliance violations and get visibility of cloud assets and resources on single Dashboard	Centralised Threats and Vulnerabilities reporting on Single Dashboard	Events or cloud operation analysed /month	5000	Event/cloud operation per month
18	Managed DdoS Protection and WAF	Web Application Firewall CSP Natively Managed	Managed service to protect Layer7 application attacks like SQL Injection with 10 WAF Rules	1 Million Request/ Month.	4	Monthly
19	Network Firewall - Cloud Native NGFW	CSP Native Managed Network Firewall - IPDS NGFW with Transport Layer	Managed Network Firewall with intrusion detection / prevention system. Each firewall endpoint will process 50 Terabyte of traffic /50 TB data processed per month , the	Monthly	4	Monthly

		Security (TLS) interception and decryption	Billing will be based on the actual consumption			
E : CSP Native Content Delivery Network (CDN)						
1	Managed CSP Native Content Delivery Network (CDN)	TB egress / data transfer out over CDN	CDN service to be used to securely deliver audio, video, images, data, application, etc., quickly by using the servers closest to each user. CDN to reduce load time and saves bandwidth.	TB per Month	4	Monthly
F : CSP Native AI/ML & Data Warehouse Platform						
1	ML Notebook	Fully managed CSP native Notebook IDE - Fully Managed & collaborative Jupyter Notebook - to perform all ML development steps (Prepare, build, Train & Deploy) from a single Web based visual interface.	Node Size 16 vCPU 64 GB RAM	Monthly	2	730
2	ML Training	Fully managed CSP native Training Jobs Service: GPU-powered instances for running training jobs. One Node - (24vCPU, 96GB of memory, 2 Nos of GPUs that supports TensorFlow, PyTorch, XgBoost ML-API for	Node Size: 24vCPU, 96 GB RAM with 2 GPUs / training job per month/730hrs	Monthly	2	730

		training Models and network performance of 32 Gbps)- Latest GPU with launch date not earlier than 2023				
3	ML Inference	Real Time Inference	Node Size 16 vCPU 64 GB RAM	Monthly	2	730
4	Fully Managed Data Warehouse	Full managed Datawarehouse with - Cloud-based enterprise data warehouse (EDW) to run complex queries across petabytes of data.	Data Warehouse Platform: a. Cloud-based enterprise Data warehouse - each unit/node having minimum configuration of 4 vCPU & 32 GB RAM, for running complex Queries(Approximate 100 Queries in Month with each query scanning of minimum of 100GB of data with 4 dedicated nodes/units for Number of units in estimated units with 100% utilization of dedicated nodes; Or b. Fully Managed Cloud-based Serverless data warehouse -should run complex queries (Approximate 100 Queries in Month with each query scanning minimum of 100GB of data for Number of units in estimated units) Pls Note: Bidder to quote only one (either a or b) option, which must support HA cluster deployment & Data Governance features including Row level Security , Data Masking, and cluster encryption using Customer Managed Key	Monthly	1	730 730
5	Managed ETL as a Service	Managed ETL Service: - Serverless service to process and transfer data between	4vCPU and 16GB	Monthly	1	730

		different compute and storage services data sources at specified intervals, create, schedule, orchestrate and manage data pipelines				
6	Data Visualization /BI Service	Fully Managed Serverless service with - Auto-scalable - Data visualization service for telemetry data and operational metrics	Data Visualization Service	Monthly	1	730
G : Generative AI As Service						
1	GenAI - Multimodal models	Multimodal Managed large model API for Image, Video, Text & Audio	Image Input/image	million/ Month	1	Monthly
2			Video Input/second	1000000	1	Monthly
3			Text Input & output - Token	million/ Month	1	Monthly
4			Audio Input/second	1000000	1	Monthly
5	Translation	Text Translation - CHAR	Text Translation (characters) in Million	million/ Month	1	Monthly
6		Text Translation - Documents	Document Translation (pages)	Number of Pages	400	Monthly
7		Speech to Text	Speech-to-Text in minutes	minutes/ Month	1000	Monthly
8	Enterprise Chat bot	Peak requests per day -Text	Number of requests per month	Request/ Month	400000	Monthly
9		Peak requests per day- Voice	Number of seconds per month	Sec/Month	50000	Monthly
10		Peak requests per day- Data Index	Amount of GB indexed per month	DB/Month	50	Monthly
11		Search LLM	LLM based Search	Request/ Month	400000	Monthly
H: MS-SQL Licenses Provided by CSP						

1	MS SQL 2017 / 2019 / 2022 Cloud based Image Licenses	Pre-configured virtual machine image with Microsoft SQL Server already installed on a Windows Server operating system. The bidder must Quote SQL core based licenses offered by CSP as pre-configured image with Windows OS & SQL server	4 vCPU, 32 GB RAM	Enterprise	2	730
2			16 vCPU, 128 GB RAM	Enterprise	2	730
3			32 vCPU, 512 GB RAM	Enterprise	2	730
4			48 vCPU, 384 GB RAM	Enterprise	2	730
5			48 vCPU, 512 GB RAM	Enterprise	3	730
6			64 vCPU, 512 GB RAM	Enterprise	2	730
7			128 vCPU, 512 GB RAM	Enterprise	15	730
8			2 vCPU, 4 GB RAM	standard	15	730
9			4 vCPU, 16 GB RAM	standard	2	730
10			2 vCPU, 8 GB RAM	web	3	730
11			2 vCPU, 16 GB RAM	web	1	730
12			4 vCPU, 4 GB RAM	web	2	730
13			4 vCPU, 8 GB RAM	web	3	730
14			4 vCPU, 16 GB RAM	web	40	730
15			8 vCPU, 16 GB RAM	web	3	730
16			8 vCPU, 32 GB RAM	web	2	730
17			8 vCPU, 64 GB RAM	web	1	730
18			16 vCPU, 16 GB RAM	web	1	730
19			16 vCPU, 32 GB RAM	web	1	730
20			16 vCPU, 64 GB RAM	web	3	730
21			32 vCPU, 32 GB RAM	web	1	730
I: One-time migration cost including 2 Month of trial operations					1	

6. Selection Criteria and evaluation process

Stage 1: Pre-Qualification

The bidder must fulfil Pre-Qualification criterion to qualify for next stage. The Bidder, not meeting any of the pre-qualification criteria, will be disqualified.

Stage 2: Technical Evaluation

1. Technical Evaluation will be done only for the bidders who qualified in Stage 1.
2. The bidders' technical solutions proposed in the bid document will be evaluated as per the requirements specified in the BID DOCUMENT and technical evaluation framework.
3. Each Technical Bid will be assigned a technical mark out of a maximum of 100 marks. Only the bidders who get a Technical score of 70% or more marks will qualify for financial evaluation stage. Failing to secure minimum marks shall lead to technical rejection of the Bid and Bidder.

Stage 3: Financial Evaluation

The financial bids for the technically qualified bidders will be opened on the notified date and time. The financial bid should **not be submitted**along with Technical Proposal.

financial evaluation will be done based on the below calculations.

The evaluation process shall consider the "Total Contract Value" Vendor proposing lowest TMO shall be given a commercial score of 30. Commercial score for other vendors will be calculated as under:

For example, if we have MSP 1, 2 and 3 quoting rates as given below:

Item	MSP 1	MSP 2	MSP 3
Total Value including taxes from Annexure XV	8,00,00,000	7,00,00,000	9,00,00,000

The overall commercial score will be determined on basis of formula given below, following which the bidder with the highest score will be awarded the contract.

- Formula

$$\frac{\text{Lowest Bid Value}}{\text{Price quoted by respective vendors}} \times 100$$

Commercial Marks (CM) x Commercial Weightage i.e., 30%

$$\text{MSP 1} = \frac{7,00,00,000}{8,00,00,000} \times 100 = 87.50 \qquad 87.5 \times 0.3 = 26.25$$

Stage 4: Final Selection

Technical and Commercial score will be added to arrive at Total Score out of hundred. The proposal securing the highest combined score will be ranked as H1, Second highest as H2 and Third Highest as H3.

Example:

As per the above example, three proposals with combined Technical and Financial evaluations score would be ranked as under:

Final evaluation based on technical score and financial score is as follows:

MSP	Tech. Marks TMW (0.7)	Commercial Marks CMW (0.3)	Total TMW + CMW	Highest Score
1	49	26.25	75.25	H2
2	52.5	30.00	82.50	H1
3	47.6	23.33	70.93	H3

Based on the above matrix the contract will be awarded to MSP 2, as MSP 2 has the highestscore (H1) of 82.5 marks.

In case there are two H1 Bidders then bid will be awarded to Bidder who quoted less financial quote.

7. Project Timelines

The bidder should follow the following project timelines:

Project Timelines

Item #	Milestone	Days
1	Issuance of Work Order to successful Bidder	T0
2	Provisioning of Cloud resources Primary Site	T0 + 30 days=T1
3	Migration of IT Application and Data from existing Service provider	T1+30 days= T2
4	Provisioning of Cloud resources DR Site	T2+ 15 days= T3
5	Mock Drill	T3+7 days= T4
5	Operation and Maintenance	Throughout the contract period

8. Support Services

- The MSP shall be responsible for providing 24*7*365 days' support to the infrastructure from the date of issuance of operational acceptance by department. Ensuring Uptime and utilization of the cloud resources as per SLA's defined in this RFP. In the event of a disaster at DC site, activation of services from the DR site is the responsibility of MSP.
- The MSP shall conduct vulnerability and penetration test (from a third-party testing agency which may be CERT-IN empaneled) on the Cloud facility every 6 months and reports should be shared with department. The MSP needs to update the system in response to any adverse findings in the report, without any additional cost to department.
- MSP is required to provision additional VMs when the utilization exceeds 80%.
- The MSP shall develop appropriate policy, checklists in line with ISO 22301, ISO 27001 and ISO 20000 framework for failover and fall back to the appropriate DR site.
- On expiration / termination of the contract, MSP shall handover complete data in the desired format to department which can be easily accessible and retrievable.

9. Contract Duration

The initial engagement period of the selected Service Provider will be 3 years from the date of issuance of Work Order, extendable for further 2 years at a time, based on the performance. During the contract period, Department and the bidder may mutually review the rates periodically based on the usage patterns and market conditions with the objective to get best of class service at least cost.

10. Pre-Bid Queries

10.1 Pre-bid meeting and Clarifications

- A pre-bid meeting will be held on as per the date mentioned in the Fact Sheet through Video Conferencing. Interested bidders must send a line of request for attending the pre-bid meeting at Email ID mentioned in the Address of Communication details in the Fact Sheet.
- Department shall invite queries from Bidders as per the details mentioned in the Fact Sheet of this document.
- The Bidders will have to ensure that their queries for Pre-Bid meeting should reach to Department by email on or before Pre-bid meeting Date mentioned in Fact Sheet of this document.
- The queries should necessarily be submitted in the following format in excel file:

Sr. No.	Section/ Page No.	Content of RFP requiring Clarifications	Change/ Clarification Requested	Remarks

- Department shall not be responsible for ensuring that the Bidder's queries have been received by them. Any requests for clarifications post the indicated date and time may not be entertained by the Department.
- The purpose of query clarification is to provide the Bidders with information regarding the RFP, project requirements, and opportunity to seek clarification regarding any aspect of the RFP and the project. However, 'Department' reserves the right to hold or re-schedule the Pre-Bid meeting.

10.2 Responses to Pre-bid Queries and Issue of Corrigendum

- The Officer notified by Department of Agriculture and Farmers Welfare will endeavor to provide timely response to the queries. However, Department makes no representation or warranty as to the completeness or accuracy of any response made in good faith, nor does Department undertake to answer all the queries that have been posed by the Bidders.
- At any time prior to the last date for receipt of bids, Department may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective Bidder, modify the RFP Document by a corrigendum.
- The Corrigendum (if any) and clarifications to the queries from all Bidders will be uploaded on the GEM portal.
- Any such corrigendum shall be deemed to be incorporated into this RFP.
- In order to provide prospective Bidders reasonable time for taking the corrigendum into account, Department may, at its discretion, extend the last date for the receipt of Proposals.

11. Payment Terms

11.1 General Payment Terms

1. The billing for cloud services will be based on actual consumption of services (Pay-As-You-Go model) with zero capital (one-time) cost.
2. Cloud Service providers will raise monthly invoices to the department.
3. Department will release the payment within 45 days of submission of valid invoice subject to the condition that invoice and all supporting documents produced are in order and work is performed as per the scope of the project and meeting the SLA Criteria.

Department shall be entitled to delay or withhold the payment of a disputed invoice or part of it delivered by MSP, when department disputes such invoice or part of it, provided that such dispute is bona fide.

4. All payments shall be made corresponding to the goods or services delivered, installed, or operationally accepted, as per the Contract Implementation Schedule, at unit prices and in the currencies specified in the Commercial Bids.
5. If the Bidder is liable for any penalty as per the SLA (refer to the related clause of this agreement), the same shall be adjusted from payments due to the Bidder.
6. In case Go-Live is delayed, the corresponding operations and maintenance phase will start after the Go-Live has been completed.

11.2 Penalty Terms for Quality of Services

For the Departments to ensure that the Cloud Service Providers or Managed Service Provider adhere to the Service Level Agreements, this section describes the Penalties which may be imposed on MSP. In case these service levels cannot be achieved at service levels defined in the agreement, the departments will invoke the performance related penalties.

The penalty in the percentage of the monthly payment has been as indicated against each SLA parameter in the table.

If outage is due to MSP except application related malfunction, then 10% penalty of month bill will be imposed.

Payments to be linked to the compliance with the SLA metrics laid down in the agreement. To illustrate calculation of penalties, an indicative example is provided below.

For ex: For SLA1 if the penalty to be levied is 7% then 7% of the Quarterly Payment is deducted from the total of the Quarterly bill and the balance paid to the MSP.

If the penalties are to be levied in more than one SLA, then the total applicable penalties are calculated and deducted from the total of the Quarterly bill and the balance paid to the MSP.

For ex: SLA1 =7% of the Quarterly Payment, SLA12=10% of the Quarterly Payment, SLA19=2% of the Quarterly Payment then, Amount to be paid = Total Quarterly bill – {(19% of the Quarterly Payment)}

Provide a robust, fault-tolerant infrastructure with enterprise-grade SLAs with an assured uptime of 99.5%, SLA measured at the VM Level and SLA measured at the Storage Levels.

The SLA for availability of Cloud service (defined as availability of all servers, storage and supporting DC infrastructure including network infrastructure and network connectivity) is 99.5% with no unscheduled downtime.

$$\frac{\text{(Total contracted minutes in a quarter – downtime during contracted minutes) * 100 Total}}{\text{contracted minutes in a quarter}}$$

In case service provider fails to achieve compliance level of services successively in two quarters or any three quarters in a year, department will reserve the right to re-look at the contract and redefine Service level agreement and penalty clauses to safeguard its interest.

11.3 Billing & Discounting Model

1. The price quoted by the bidder for each line item in the commercial bid format will be frozen for entire contract period.
2. The billing for each line item should be calculated either based on the quoted price or the current public pricing (after applying discount), whichever is lower as on billing date.
3. The bidder should provide the discount percentage on each category as mentioned in BOM. These discounts would remain firm for the entire contract period.
4. The Discount provided as part of this bid document will be used to procure any additional service or configuration of service in the host of offerings of the CSP at the same rate of discount. The services used which do not belong to any category A, B and C, the discount will be calculated based on the category "D".
5. To facilitate evaluation of bids, the Department of Agriculture and Farmer Welfares', at its sole discretion, may seek clarification in writing regarding the bid.
6. The Department of Agriculture and Farmer Welfares' may review the price/cost quoted periodically in view of various factors including but not limited to significant price/cost reduction for same services in market.
7. Final choice of firm for the project shall be made on the basis of conformity to eligibility, technical proposal and appropriateness of the financial offer from the point of view of cost effectiveness over the entire period for the services and capability of the firm to execute and service the project.

12. Service Level Agreement

- The purpose of Service Levels is to define the levels of service provided by the Cloud Service Provider ("MSP") to the Department for the duration of the contract. The benefits of this are:
    - Help the Client control the levels and performance of MSP's services.
    - Create clear requirements for measurement of the performance of the system and help in monitoring the same during the Contract duration.
- The Service Levels are between the Department and MSP.

12.1 Service Level Agreements and Targets

- This section is agreed to by Client and MSP as the key performance indicator for the project.
- The following section reflects the measurements to be used to track and report system's performance on a regular basis. The targets shown in the following tables are for the period of Contact.

12.2 General Principles of Service Level Agreements

Service Level Agreement (SLA) shall become the part of the Contract between the Client and the MSP. SLA defines the terms of MSP's responsibility in ensuring the timely delivery of the services and the correctness of the services based on the agreed performance indicators as detailed in this section.

The MSP shall comply with the SLAs to ensure adherence to project quality and availability of services throughout the duration of the Contract. For the purpose of the SLA, definitions and terms as specified in the document along with the following terms shall have the meanings set forth below:

"Total Time" – Total number of hours in the quarter being considered for evaluation of SLA performance.

"Downtime" – Time period for which the specified services/components/system are not available in the concerned period, being considered for evaluation of SLA, which shall exclude downtime owing to Force Majeure and reasons beyond control of the MSP.

"Scheduled Maintenance Time"– Time period for which the specified services/components/system with specified technical and service standards are not available due to scheduled maintenance activity. The MSP shall seek at least

15 days' prior written approval from the Client for any such activity. The scheduled maintenance shall be carried out during non-peak hours and shall not exceed more than four (4) hours and not more than four (4) times in a year.

"Uptime" – Time period for which the specified services are available in the period being considered for evaluation of SLA.

Uptime (%) = (1- {[Total Downtime] / [Total Time- Scheduled Maintenance Time]}) * 100. Penalties shall be applied for each criterion individually and then added together for the total penalty for a particular quarter

"Incident" – Any event/abnormalities in the service/system being provided that may lead to disruption in regular/normal operations and services to the end user.

"Response Time" – Time elapsed from the moment an incident is reported to the Helpdesk either manually or automatically through the system to the time when a resource is assigned for the resolution of the same.

"Resolution Time" – Time elapsed from the moment incident is reported to the Helpdesk either manually or automatically through system, to the time by which the incident is resolved completely and services as per the Contract are restored.

"Target" – is the availability of cloud and managed services and their data. It is calculated as = [(Total uptime of all cloud and managed services in a quarter)/ (Total time in quarter)] *100.

Latency: Latency may address the storage and the time when the data is placed on mirrored storage.

Maximum Data Restoration Time: refers to the committed time taken to restore cloud service customer data from a backup.

Recovery Point Objective: It is the maximum allowable time between recovery points. RPO does not specify the amount of acceptable data loss, only the acceptable time window. RPO affects data redundancy and backup.

Recovery Time Objective: It is the maximum amount of time a business process may be disrupted, after a disaster, without suffering unacceptable business consequences. Cloud services can be critical components of business processes.

Availability of Reports (Reports such as Provisioning, Utilization Monitoring Reports, User Profile Management etc.)

Penalty shall be applied for each criterion individually as per downtime of each applicable component and then added together for the total penalty for a particular quarter.

12.3 Service Levels Monitoring

- The Service Level parameters shall be monitored on a quarterly basis. Penalties associated with performance for SLAs shall be made after deducting from applicable payments of the quarter or through the Performance Bank Guarantee.
- As part of the Project requirements, MSP shall supply and make sure of appropriate system (software/hardware) to automate the procedure of monitoring SLAs during the course of the Contract and submit reports for all SLAs as mentioned in this section. This software along with any system specific software shall be used by the MSP for monitoring and reporting these SLAs. The Client reserves the right to test and audit these tools for accuracy and reliability at any time. If at any time during the test and audit the accuracy and reliability of tools shall be found to be compromised, the Client reserves the right to invoke up to double the penalty of the respective quarterly phase.
- The MSP will endeavor to exceed these levels of service wherever possible.
- MSP undertakes to notify the Client of any difficulties, or detrimental/adverse findings as soon as possible once they are identified.
- MSP will provide a supplemental report on any further information received, as soon as the information becomes available.
- MSP will take instruction only from authorized personnel of the Client.
- In case issues are not rectified to the complete satisfaction of Client, within a reasonable period of time defined in the RFP, the Client shall have the right to take appropriate remedial actions including liquidated damages, applicable penalties, or termination of the Contract.
- For issues i.e., breach of SLAs beyond control of the MSP, the MSP shall submit a justification for the consideration of the Client. In case it is established that the MSP was responsible for such breach, respective penalty shall be applied to the MSP.
- In case if any of the information mentioned in the further measurements of services does not match the SLA as per MeitY, then the SLA measurements mentioned in the MeitY guidelines will be final.

12.4 Measurements and Targets – Operations Phase SLAs

- These SLAs shall be used to evaluate the performance of the services post the Implementation Phase and during the operations Phase. These SLAs and associated performance shall be monitored on a quarterly basis. Penalty levied for non-performance as per SLA shall be deducted through subsequent payments due from the Client or through the Performance Bank Guarantee.
- The Scheduled Maintenance Time shall be agreed upon with the Client as per the definition given as part of this section of the Contract.
- MSP's published SLAs and penalties shall be also being applicable during the course of the Contract.
- The following SLAs apply both for MSP and MSP/SI. While the MSP will be responsible for maintaining the SLAs pertaining to the cloud infrastructure, network, controls etc., the MSP will be responsible for the SLAs related to managing and monitoring the cloud services

#	Service Level Objective	Measurement Methodology	Target/Service Level	Penalty (Indicative)
Availability/Uptime				
1	Availability/Uptime of cloud servic es Resources for Production environment (VMs, Storage, OS, VLB, Security Components,)	Availability (as per the definition in the SLA) will be measured for each of the underlying components (e.g., VM, Storage, OS, VLB, Security Components) provisioned in the cloud.	Availability for each of the provisioned resources: >=99.5%	Default on any one or more of the provisioned resources will attract penalty as indicated below. =<99.5% - >=99% (10% of the <MP>) < 99% (30% of the <MP>)
2	Availability of Critical Services (e.g., Register Support Request or Incident; Provisioning / De-Provisioning; User Activation / Deactivation; User Profile Management; Access Utilizatio n Monitoring Reports) over User / Admin Portal and APIs (where applicable)	Availability (as per the definition in the SLA) will be measured for each of the critical services over both the User / Admin Portal and APIs (whe re applicable)	Availability for each of the critical services over both the User / Admin Portal and APIs (where applicable) >= 99.5%	Default on any one or more of the services on either of the portal or APIs will attract penalty as indicated below. =<99.5% - >=99% (10% of the <MP>) < 99% (20% of the <MP>)
3	Availability of the network links at DC and DR (links at DC / DRC, DCDRC link)	Availability (as per the definition in the SLA) will be measured for each of the network links provisioned in the	Availability for each of the network links: >= 99.5%	Default on any one or more of the provisioned network links will attract penalty as indicated below. =<99.5% - >=99% (10% of

#	Service Level Objective	Measurement Methodology	Target/Service Level	Penalty (Indicative)
		cloud.		the <MP>) < 99% (30% of the <MP>)
4	Availability of Regular Reports (e.g.,Audit, Certifications,) indicating the compliance to the Provisional Empanelment Requirements.		15 working days from the end of the quarter. If STQC issues a certificate based on the audit, then this SLA is not required.	5% of MP

Support Channels – Incident and Helpdesk				
5	Response Time	Average Time taken to acknowledge and respond once a ticket/incident is logged through one of the agreed channels. This is calculated for all tickets/incidents reported within the reporting month.	95% within 15minutes	<95% and >=90% (5% of the MP) < 90% and >= 85% (7% of the MP) < 85% and >= 80% (9% of the MP)
6	Time to Resolve – Severity 1	Time taken to resolve the reported ticket/incident from the time of logging.	For Severity 1, 98% of the incidents should be resolved within 30 minutes of problem reporting	<98% and >=90% (5% of the MP) < 90% and >= 85% (10% of the MP) < 85% and >= 80% (20% of the MP)
7	Time to Resolve – Severity 2,3	Time taken to resolve the reported ticket/incident from the time of logging.	95% of Severity 2 within 4 hours of problem reporting and 95% of Severity 3 within 16 hours of problem reporting	<95% and >=90% (2% of the MP) < 90% and >= 85% (4% of the MP) < 85% and >= 80% (6% of the MP)
Security Incident and Management Reporting				
8	Percentage of timely	Measured as a percentage by the	95% within 1	<95% and >=90% (5% of

#	Service Level Objective	Measurement Methodology	Target/Service Level	Penalty (Indicative)
	incident report	number of defined incidents reported within a predefined time (1 hour) limit after discovery, over the total number of defined incidents to the cloud service which are reported within a predefined period (i.e., month). Incident Response – MSP shall assess and acknowledge the defined incidents within 1 hour after discovery.	hour	the MP) < 90% and >= 85% (10% of the MP) < 85% and >= 80% (15% of the MP)
9	Percentage of timely incident resolutions	Measured as a percentage of defined incidents against the cloud service that are resolved within a predefined time limit (month) over the total number of defined incidents to the cloud service within a predefined period. (Month). Measured from Incident Reports	95% to be resolved within 1 hour	<95% and >=90% (5% of the MP) < 90% and >= 85% (10% of the MP) < 85% and >= 80% (15% of the MP)
Vulnerability Management				
10	Percentage of timely vulnerability corrections	The number of vulnerability corrections performed by the cloud service provider – Measured as a percentage by the number of vulnerability corrections performed within a predefined time limit, over the total number of vulnerability	99.95%	>=99% and <99.95% (10% of the MP) >=98% and <99% (20% of the MP) <98% (30% of the MP)

#	Service Level Objective	Measurement Methodology	Target/Service Level	Penalty (Indicative)
		corrections to the cloud service which are reported within a predefined period (i.e., month, week, year, etc.). • High Severity Vulnerabilities – 30 days – Maintain 99.95% service level • Medium Severity Vulnerabilities – 90 days – Maintain 99.95% service level		
11	Percentage of timely vulnerability reports	Measured as a percentage by the number of vulnerability reports within a predefined time limit, over the total number of vulnerability reports to the cloud service which are reported within a predefined period (i.e., month, week, year, etc.).	99.95%	>=99% and <99.95% (10% of the MP) >=98% and <99% (20% of the MP) <98% (30% of the MP)
Vulnerability Management				
12	Security breach including Data Theft/Loss/Corruption	Any incident where in system compromised or any case wherein data theft occurs (including internal incidents)	No breach	For each breach/data theft, penalty will be levied as per following criteria. Any security incident detected INR << 5 Lakhs>>.This penalty is applicable per incident. These penalties will not be part of overall SLA penalties cap per month. In case of serious breach of security wherein the data is stolen or corrupted, Government Department reserves the right to terminate the contract

13	Availability of SLA reports covering all		(e.g., 3 working days from the	5% of MP

#	Service Level Objective	Measurement Methodology	Target/Service Level	Penalty (Indicative)
	parameters required for SLA monitoring within the defined time		end of the month)	
Service levels DR				
14	Recovery Time Objective (RTO) (Applicable when taking Disaster Recovery as a Service from the Service Provider)	Measured during the regular planned or unplanned (outage) changeover from DC to DR or vice versa.	<<= 2 hours>> [Government Department / Agency to indicate based on the application requirements]	10% of MP per every additional 1 (one) hour of downtime
15	Recovery Point Objective (RPO) (Applicable when taking Disaster Recovery as a Service from the Service Provider)	Measured during the regular planned or unplanned (outage) changeover from DC to DR or vice versa.	<= 30mins [Government Department / Agency to indicate based on the application requirements]	10% of MP per every additional 30 (thirty) mins of downtime
16	Availability of Root Cause Analysis (RCA) reports for Severity 1 and 2		Average within 5 Working days	5% of MP

Note: MP means Monthly Payment Share of that quarter

12.5 Severity Level

Below severity definition provide scenarios for incidents severity.

Severity Level	Description	
Severity 1	More than 50% users affected for more than one hour	
Severity 2	More than 25% and upto 50% users affected for more than 2 hour	
Severity 3	Upto 25% of users affected for more than 4 hours.	

13. Special Terms and Condition

13.1 Definition of Terms

- The Contract' means the agreement entered into between department and Contractor as per the Contract Agreement signed by the parties, including all attachments and appendices there to and all documents incorporated by reference therein.
- 'Owner' or "Department" shall mean the Department of Agriculture and Farmers' Welfare Ministry of Agriculture and Farmers' Welfare Government of India having its corporate office at 026A, Ground Floor, Krishi Bhawan, Delhi, India – 110001 and shall include their legal representatives, successors, and assigns.
- 'Contractor' or 'Manufacturer' shall mean the Bidder whose bid will be accepted by the department for the award of the Works and shall include such successful Bidder's legal representatives, successors and permitted assigns.
- 'Sub-Contractor' shall mean the person named in the Contract for any part of the Works or any person to whom any part of the Contract has been sublet by the Contractor with the consent in writing of the Engineer and will include the legal representatives, successors and permitted assigns of such person.
- 'Engineer' shall mean the officer appointed in writing by the department to act as Engineer from time to time for the purpose of the Contract by the department.
- 'Consulting Engineer'/ 'Consultant' shall mean any firm or person duly appointed as such from time to time by the department.
- The terms 'Equipment', 'Stores', and 'Materials' shall mean and include equipment, stores and materials to be provided by the Contractor under the Contract.
- 'Works' shall mean and include the furnishing of equipment/materials at site and if required, supervision of unloading, storage, handling at site, erection, testing and commissioning and putting into satisfactory operation as defined in the Contract.
- 'Specifications' shall mean the Specifications and Bidding Document forming a part of the Contract and such other Schedules and drawings as may be mutually agreed upon.
- 'Site' shall mean and include the land and other places on, into or through which the Works and the related facilities are to be erected or installed and any adjacent land, paths, street or reservoir which may be allocated or used by the department or Contractor in the performance of the Contract.
- The term 'Contract Price' shall mean the lump sum price quoted by the Contractor in his bid with additions and/or deletions as may be agreed and incorporated in the Letter of Award, for the entire scope of the works.
- 'Manufacturer's Works' or 'Contractor's Works' shall mean the place of Works used by the manufacturer, the Contractor, their collaborators/associates, or Sub-Contractors for the performance of the Contract.
- 'Inspector' shall mean the department, or any person nominated by the department from time to time, to inspect the equipment, stores or Works under the Contract and/or the duly authorized representative of the department.
- 'Notice of Award of the Contract' / 'Letter of Award' / 'Telex of Award' shall mean the official notice issued by the department notifying the Contractor that his bid has been accepted.
- 'Date of Contract' shall mean the date on which Notice of Award of Contract/Letter of award has been issued.
- 'Month' shall mean the calendar month. 'Day' or 'Days' unless herein otherwise expressly defined shall mean calendar day or days of 24 hours each.
- A 'Week' shall mean continuous period of 7 (seven) days.
- 'Writing' shall include any manuscript, type written or printed statement, under or over signature and/or seal as the case may be.
- When the words 'Approved', 'Subject to Approval', 'Satisfactory', 'Equal to', 'Proper',' 'Requested', 'As Directed', 'Where Directed', 'When Directed', 'Determined by', 'Accepted', 'Permitted', or words and phrases of like importance are used the approval, judgment, direction etc., is understood to be a function of the department /Engineer.
- Test on completion shall mean such tests as prescribed in the Contract to be performed by the Contractor before the work is taken over by the department.
- "Startup" shall mean the time period required to bring the equipment covered under the Contract from an inactive condition, when construction is essentially completed, to the state ready for trial operation. The startup period shall include preliminary inspection and checkout of equipment and supporting subsystem, initial operation of the complete equipment covered under the Contract to obtain necessary pretrial operation data, perform calibration and corrective action, shut down, inspection and adjustment prior to the trial operation period.
- 'Initial operation' shall mean the first integral operation of the complete equipment covered under the Contract with the sub-system and supporting equipment in service or available for service.
- 'Trial operation', 'Reliability Test', 'Trial Run', 'Completion test', shall mean the extended period of time after the startup period. During this trial operation period the unit shall be operated over the full load range. The length of Trial Operation shall be as determined by the Engineer, unless otherwise specified elsewhere in the Contract.
- 'Performance and Guarantee Test' shall mean all operational checks and tests required to determine and demonstrate capacity, efficiency, and operating characteristics as specified in the Contract Documents.
- The term 'Final Acceptance' shall mean the department's written acceptance of the Works performed under the Contract, after successful commissioning/completion of Performance and Guarantee Tests, as specified in the accompanying Technical Specifications or otherwise agreed in the Contract.
- 'Commercial Operation' shall mean the condition of operation in which the complete equipment covered under the Contract is officially declared by the department to be available for continuous operation at different loads up to and including rated capacity. Such declaration by the department, however, shall not relieve or prejudice the Contractor of any of his obligations under the Contract.

- 'Warranty Period'/ 'Maintenance Period' shall mean the period during which the Contractor shall remain liable for repair or replacement of any defective part of the Works performed under the Contract.
- 'Latent Defects' shall mean such defects caused by faulty design, material or workmanship which cannot be detected during inspection, testing etc. based on the technology available for carrying out such tests.

13.2 Bid Price

- The Bidder shall quote firm price valid till the complete execution of order mentioned in the total contract price on the GeM portal.
- All rates and amount shall be indicated in Indian rupees only.
- The maintenance charges, if any, quoted shall be inclusive of all cost (details indicated in DTS- Detailed Technical Specifications).
- All inclusive (including taxes) prices are to be submitted on GeM portal.

13.3 Taxes and Duties

- All the Bidders are requested to familiarize themselves with the laws, rules and regulations prevailing in India and consider the same while developing and submitting their Proposal.
- All Customs duties, Excise Duties, GST, and other levies payable by the bidder on goods, equipment's, components, Sub-assemblies, raw materials and any other items used for their consumption or dispatched directly to department by the contractor, or their sub-suppliers shall be included in the bid price and any such taxes, duties, levies additionally payable will be to bidder's account and no separate claim on this account will be entertained by the department.
- The Contractor shall be liable and pay all non-Indian taxes, duties, levies, lawfully assessed against the department or the Contractor in pursuance of the Contract. Tax liability, if any, on Contractor's personal income and property shall be borne by the Contractor and shall be the responsibility of the Contractor as per Tax Laws of India.
- Department shall be entitled to deduct applicable tax (if any) at source as per Indian Laws from all payments due to the Contractor under the contract.
- As regards the Indian Income Tax, surcharges on Income Tax and any other corporate tax, department shall not bear any tax liability, whatsoever, irrespective of the mode of contracting. The Contractor shall be liable and responsible for payment of all such taxes, if attracted under the provisions of the law. In this connection, attention of Contractors is invited to the provisions of Indian Income Tax Act and the circulars issued by the Central Board of Direct Taxes, Government of India.
- If any rates of taxes/duties/levies (hereinafter called 'Tax') are increased or decreased, a new Tax is introduced, an existing Tax is abolished or any change in interpretation or application of any Tax occurs in the course of the performance of Contract, which was or will be assessed on the Contractor in connection with performance of the Contract, an equitable adjustment of the Contract Price shall be made to fully take in to account any such change by addition to the Contract Price or deduction there from, as the case may be. However, these adjustments would be restricted to direct transactions between the department and the Contractor and not on procurement of components/products/services etc. by the Contractor and shall also not be applicable on the bought- out items dispatched directly from sub vendor's works to site.

13.4 Insurance

The seller at his cost shall arrange, secure, and maintain all insurance as may be pertinent and obligatory in terms of law to protect his interest and interests of the department against all perils. The responsibility to always maintain adequate insurance coverage till the completion of the work shall be of Seller alone. The insurance covers to be taken by the seller shall be in the name of department. The seller shall however be authorized to deal directly with the insurance company.

13.5 Validity of Bids

Bids will remain valid and open for acceptance as specified in the GeM portal. Prior to the expiry of the period of Bid validity prescribed by the Purchaser, the Purchaser will notify the successful bidder on GeM portal. Successful bidder shall accept the same on GeM portal within required time as per the terms and Conditions.

13.6 Process to be Confidential

Any effort by a bidder to influence the Purchaser in the process of examination, clarification, evaluation, and comparison of Bids, and in decisions concerning the award of Contract, may result in the rejection of his Bid.

13.7 Cost of Bidding

All the costs and expenses incidental to preparation and submission of the proposals, discussions including pre-award discussions with the successful Bidder etc. shall be to the account of the Bidders and the department shall not be responsible in any way whatsoever, and shall bear no liability whatsoever, on such costs and expenses, regardless of the conduct or outcome of the Bidding process.

13.8 Earnest Money of Deposit (EMD)

As mentioned in the Fact Sheet

13.9 Modification and Withdrawal of Bids

- A Bid valid for a shorter period may be rejected by the department as non-responsive.

- No bid may be modified subsequent to the deadline for submission of bids.
- No bid may be withdrawn in the interval between the deadline for submission of bids and the expiration of the period of bid validity specified by the Bidder on the Bid Form. Withdrawal/modification of a bid during this interval may result in the forfeiture of bid security.

13.10 Information required of the Proposal

The following information shall be required with technical bid in the form of scanned copies, if required.

- The complete information shall be provided by the Bidder in the form of separate sheets, drawing, catalogues, etc.
- Oral statements made by the Bidder at any time regarding quality, quantity or arrangement of the equipment or any other matter will not be considered.
- Standard catalogue pages and other documents of the Bidder may be used in the bid to provide additional information and data as deemed necessary by the Bidder.
- In case the 'Bid Proposal' information contradicts RFP requirements, the RFP requirements will govern, unless otherwise brought out clearly in the technical/commercial deviation schedules.

13.11 Document Comprising the Bid

The Bidder shall complete all the e-Bid Forms inclusive of Price Schedules, Schedule of Requirements etc. furnished in the RFP, indicating, for the products to be supplied and services to be rendered, a brief description of products and services, quantities and prices.

The Bidder shall also upload documentary evidence to establish that the Bidder meets the Qualifications Requirements as detailed in clause.

13.12 Scope of Proposal

The scope of the proposal shall be based on a sole responsibility of the bidder, completely covering all the materials and services specified under the accompanying RFP documents.

13.13 Format and Signing of Bid

- The Bidder shall complete all the procedure and format of the bid.
- The bid must contain the name and place of business of the person or persons making the bid and must be signed by the Bidder with his usual signature as per Terms and Conditions. The names of all persons signing should also be typed or printed below the signature.
- Bids by Corporation/Company must be signed with the legal name of the Corporation/Company by the President, Managing Director or by the Company Secretary or other person or persons authorized to bid on behalf of such Corporation/Company in the matter.
- Satisfactory evidence of authority of the person signing on behalf of the Bidder shall be furnished with the bid.
- The Bidder's name stated on the proposal shall be the exact legal name of the firm.
- Bids not confirming to the above requirements of Clause may be disqualified.

13.14 Bid Submission

The Bidder shall submit the entire bids on GeM portal within the deadline. The bids are to be uploaded on above portal in two parts i.e., Technical Bid and Financial Bid. This may also include all the technical details along with scanned EMD (if applicable) and unpriced BOQ on the portal.

The department may, at its discretion, extend this deadline for the submission of bids by amending the Invitation to Bid/ RFP, in which case all rights and obligations of the department and Bidders previously subject to the deadline will thereafter be subject to the deadline as extended.

If required any brochures/specifications relating to items in such case their scan copy to be uploaded in technical bids.

13.15 Opening of Bids by the Department

The Bids shall be opened by the department on bid opening date and time as specified in Invitation of bids or in the case any extension has been given thereto, after the extended Bid submission date notified on the portal.

The Bidders' names, bid prices, modifications, bid withdrawals and the presence or absence of the requisite bid guarantee and such other details as the department, at its discretion may consider appropriate, will be announced at the opening.

No electronic recording devices will be permitted during bid opening.

13.16 Preliminary examination

- The department will examine the bids to determine whether they are complete, whether required

bid security has been furnished, whether bidder fulfils the qualifying requirements and whether the bids are generally in order.

- Prior to detailed evaluation, the department will determine the substantial responsiveness of each bid with reference to the bidding documents. A substantial responsive bid is one which confirms to all the terms and conditions of the bidding documents without material deviation. The department's determination of bids responsiveness will be based on the contents of the bid itself.
- A bid determined as not substantially responsive will be rejected by the department and may not subsequently be made responsive by the bidder by correction of the non-conformity.
- The department may waive any minor informality or non-conformity or irregularity in a bid which does not constitute a material deviation. The decision of the department with regards to the deviation being material or not shall be final and binding.
- The Bidder should ensure that the prices furnished in various price schedules are consistent with each other. In the case of any inconsistency in the prices, furnished in the specified price schedules to be identified in Bid Form for this purpose, the department shall be entitled to consider the highest price for the purpose of evaluation and for the purpose of award of Contract use the lowest of the prices in these schedules.

13.17 Evaluation of Bid

- The department will evaluate and compare the Bids previously determined to be substantially responsive pursuant to Preliminary examination.
- The Bids submitted by the Bidders which do not meet the qualifying requirements as per will be treated as non-responsive and will be rejected.
- The Bids shall be evaluated and compared as per the entire Scope of Work defined in the Detailed Technical Specifications.

13.18 Award of Work

- Notification of Award of Contract on the portal will be made in writing by registered post or by hand to the successful Bidder by the department. The notification of award shall constitute the formation of Contract.
- On account of indivisible nature of work, contract will be awarded on single responsibility basis only as per outcome of evaluation process mentioned in the RFP.
- The department reserves the right, to accept any Bid (not necessarily the Bid having lowest Bid prices) or to reject any or all Bids or to cancel/withdraw the Invitation to Bid or to annul the Bidding process at any time prior to Award of Contract, without assigning any reason for such decision. Such decision by the department shall not be subject to question by any Bidder and the department shall bear no liability whatsoever consequent upon such a decision nor shall he have any obligation to inform the affected Bidder or Bidders of the grounds for the department's action.
- The department reserves the right to accept or reject any e-Bid and to annul the e-bidding process and reject all e-Bids at any time prior to award of Contract, without thereby incurring any liability to the affected bidder or bidders or any obligation to inform the affected bidders or bidders of the grounds for the Purchaser's action.

13.19 Indemnification

- Bidder shall indemnify, protect and save DA&FW and hold DA&FW harmless from and against all claims, losses, costs, damages, expenses, action suits and other proceedings, (including reasonable attorney fees), relating to or resulting directly or indirectly from
- i. an act or omission of the Bidder, its employees, its agents, or employees of the consortium in the performance of the services provided by the Bidder
- ii. breach of any of the terms of this RFQ or breach of any representation or warranty by the Bidder
- iii. Use of the deliverables and or services provided by the Bidder
- iv. Infringement of any patent trademarks copyrights etc. or such other statutory infringements in respect of all components provided to fulfil the scope of this project. Bidder shall further indemnify DA&FW against any loss or damage to DA&FW's premises or property, DA&FW's data, direct financial loss, loss of life, etc., due to the acts of the Bidder's employees or representatives. The Bidder shall further indemnify DA&FW against any loss or damage arising out of loss of data, claims of infringement of third- party copyright, patents, or other intellectual property, and third-party claims on DA&FW for malfunctioning of the equipment or software or deliverables at all points of time, provided however,
- a. DA&FW notifies the Bidder in writing in a reasonable time frame on being aware of such claim
- b. The Bidder has sole control of defence and all related settlement negotiations
- c. DA&FW provides the Bidder with the assistance, information and authority as it deems fit to perform the above
- • It is clarified that the Bidder shall in no event enter into a settlement, compromise or makes any statement (including failure to take appropriate steps) that may be detrimental to the DA&FW's (and/ or its customers, users and service providers) rights, interest and reputation.
- • Bidder shall be responsible for any loss of data, loss of life, etc., due to acts of Bidder's representatives, and not just arising out of gross negligence or misconduct, etc., as such liabilities pose significant risk.
- • Bidder should take full responsibility for its and its employee's actions. Further, since the DA&FW's data could be integrated/ used under Bidder provided software, the Bidder should be responsible for loss/ compromise or damage to DA&FW's data and for causing reputation risk to DA&FW.
- • The Bidders should indemnify DA&FW (including its employees or representatives) from and against claims, losses, liabilities, penalties, fines and suits arising from:

- i. IP infringement under any laws including Copyrights Act 1957 & IT Act 2000 and 2021 (& its amendments), Digital Personal Data Protection Act 2023 and such other statutory acts and amendments thereto
- ii. Negligence and misconduct of the Bidder, its employees, and agents
- iii. Breach of any terms of RFQ, Representation or Warranty
- iv. Act or omission in performance of service
- v. Loss of data due to any of the reasons mentioned above
- vi. Non-compliance of the Bidder with Laws/ Governmental/ regulatory Requirements
- • In the event that DA&FW is called as a defendant for IPR infringement of patent, trademark or industrial design rights arising from use of any of the components of the supplied solution, the Bidder on its own expense will undertake to defend DA&FW.
- • It will be the Bidder's responsibility to rapidly do away with third-party claims. The Bidder will also pay any compensation arising from the infringement claims and DA&FW will in no manner be responsible for such payments. In addition, the Bidder will bear all the related expenses and legal fees.
- • On its part, DA&FW will immediately relay to the Bidder any such claims and offer assistance within reasonable limits to rid the claim.
- • The Bidder claims and represents that it has obtained appropriate rights to provide the Deliverables and Services upon the terms and conditions contained in this RFQ.
- i. The Bidder shall be responsible at its own cost for obtaining all necessary authorizations and consents from third party licensors of Software used by Bidder in performing its obligations under this Project.
- ii. If a third party's claim endangers or disrupts DA&FW's use of the Deliverables, Bidder shall at no further expense, charge, fee or cost to DA&FW, obtain a license so that DA&FW may continue use of the Deliverables in accordance with the terms of this RFQ.
- iii. Bidder shall indemnify and keep fully and effectively indemnified DA&FW from all legal actions, claims, or damages from third parties arising out of use of software, designs or processes used by Bidder or their subcontractors or in respect of any other services rendered under this RFQ.

13.20 Force Majeure

The Bidder or DA&FW shall not be responsible for delays or non-performance of any or all contractual obligations, caused by war, revolution, insurrection, civil commotion, riots, mobilizations, strikes, blockade, acts of God, plague or other epidemics, earthquakes, fire, flood, obstructions of navigation by ice of Port of dispatch, acts of government or public enemy or any other event beyond the control of either party, which directly, materially and adversely affect the performance of any or all such contractual obligations.

If a Force Majeure situation arises, the Bidder shall promptly notify DA&FW in writing of such conditions and any change thereof. Unless otherwise directed by DA&FW in writing, the Bidder shall continue to perform their obligations under the contract as far as possible and shall seek all means for performance of all other obligations, not prevented by the Force Majeure event.

13.21 If the duration of delay due to force majeure continues beyond a period of three months, Vendor and DA&FW shall hold discussion to find a solution. However, notwithstanding the above, the decision of DA&FW would be final and binding on the Vendor.Patent Rights and Intellecutal Property Rights

13.22 Royalties and fees for patents covering material/equipment or process used in executing the work shall be to the account of the Vendor. The Vendor shall satisfy all demands that may be made any time for such royalties and fees and he alone shall be liable for damages, infringement and shall keep the purchase indemnified in that regard. In the event, any equipment's/material or part thereof supplied by the Vendor is involved in any suit or other proceedings held to constitute infringements, and its use is enjoyed, the Vendor, shall at his own expenses, either procure for the purchaser the right to continue the use of such equipment/material or replace it with a non-infringing material/equipment/or modify it so that it becomes non-fringing.

13.23 The Department (Client) shall retain full ownership of all intellectual property (IP) related to its data, content, and any custom developments made under this agreement. The MSP shall have a non-exclusive, royalty-free license to use any IP provided by the Department solely for the purpose of delivering the cloud services. The MSP shall ensure that the Department's data and IP are protected from unauthorized use or disclosure. Any third-party IP incorporated into the services will be licensed to the Department as necessary for service delivery. Upon contract termination, the Department's IP and data shall be returned or securely deleted, as per the terms of the agreement.Fraud and Corrupt Practices

The MSP agrees to adhere to the highest standards of integrity and ethics while executing this agreement. The Department will not tolerate any form of fraud, corruption, coercion, or unethical behavior, including offering, giving, receiving, or soliciting bribes, kickbacks, or any inducements. In case of detection of such practices, the Department reserves the right to terminate the contract, blacklist the MSP, and take legal action. The MSP shall also ensure that its employees and subcontractors comply with these standards.

13.24 Disputes and Arbitration

- The department and Service provider shall make every effort to resolve amicably by direct informal negotiation, any disagreement or dispute arising between them under or in connection with the Contract.
- If after thirty (30) days from the commencement of such internal negotiations, the department and Service provider have been unable to resolve amicably a contract dispute; either party may require that the dispute be referred for resolution to

the formal mechanism specified below.

- In the case of dispute between the department and service provider the dispute shall be referred to adjudication/ arbitration in accordance with Indian Laws.
- The award given by the Arbitrator(s) shall be speaking award.

13.25 Operational Acceptance

Operational Acceptance shall be provided by the department only after.

- Working of application from primary site
- Complete Data Replication and Reverse Data Replication as per RPO
- Switch over of application from DC to DR as per defined RTO and RPO
- Switch back of applications from DR to DC as predefined RTO and RPO
- Fully functional application while DR site is operational, taking into consideration the end user experience

13.26 Extension of Contract

Department has the option to extend the tenure of the contract for continuation of the services. The duration of extension will be decided by department and will be up to a minimum of two years. The decision on the extension will be taken by department keeping in consideration of:

- Satisfactory performance of the MSP
- Technological reasons
- Where circumstances unavoidably require taking recourse to this option.

13.27 Project Planning and Management

The success of the project depends on the proper project planning and management. At the onset, the Bidder shall plan the project implementation in great details and should provide a micro level view of the tasks and activities required to be undertaken in consultation with department. An indicative list of planning related documentation that the Bidder should make at the onset is as follows:

- Project Schedule: A detailed week-wise timeline indicating various activities to be performed along with completion dates and resources required for the same
- Manpower Deployment List: A list needs to be provided with resources who will be deployed on the project along with the roles and responsibilities of each resource.
- Resource Deployment List: List and number of all cloud-based resources (including but not limited to servers (VMs), storage, network components and software components) other than manpower that may be required.
- Communication Plan: Detailed communication plan indicating what form of communication will be utilized for what kinds of meeting along with recipients and frequency.
- Migration Plan: The Bidder will be required to submit a migration plan to department for migrating the application on its Cloud. Necessary support will be provided by the application vendor of department.
- Progress Monitoring Plan and Reporting Plan: Detailed Daily, Weekly, Monthly Progress Report formats along with issue escalation format. The format will be approved by department to the successful bidder before start of the project.
- Standard Operating Procedures: Detailed procedures for operating and monitoring the Cloud site.
- Risk Mitigation Plan: List of all possible risks and methods to mitigate them.
- Escalation Matrix and Incident Management: A detailed list of key contact persons with contact details with escalation hierarchy for resolution of issues and problems. This has to be via an Incident Management system.
- Training Strategy: The training strategy should be designed to provide training to the IT technical team personnel identified by department. Department will measure the effectiveness after the completion of the training through training feedback forms. A formal training plan with relevant course material is required as part of the training session.

13.28 Disaster Recovery and Business Continuity Services

In addition to the Primary DC, the MSP is responsible for Disaster Recovery Services to ensure continuity of operations in the event of failure of the primary data center and meet the RPO and RTO requirements. However, during the change from DC to DRC or vice-versa (regular planned changes), there should not be any data loss. There shall be asynchronous replication of data between Primary DC and DRDC and the MSP has been responsible for sizing and providing the DC-DR replication link to meet the RTO and the RPO requirements.

The Primary DC and the DR should be in different seismic zones.

- The DRC can be offered from a traditional Data Center Facility and all the relevant mandatory requirements defined for the Primary Data Center as indicated below apply for the Disaster.
- Recovery Center:
    a. Deployment Model Specific Requirements
    b. General Requirements
    c. Service Level Agreement Management
    d. Operational Management

e. Data Management
f. User/Admin Portal Requirements
g. Integration Requirements
h. LAN / WAN Requirements
i. Data Center Facilities Requirements
j. Security Requirements
k. Legal Compliance Requirements
l. Management Reporting Requirements
m. Exit Management and Transition Requirements

- In case of any disaster, the security posture of the DR site shall be identical to the posture provided in the DC.
- The disaster recovery site shall have a similar environment (physical and IT), processes, and controls (security, etc.) as that of the primary DC. During normal operations, the Primary Data Center has been serving the requests. The Disaster Recovery Site has been not be performing any work but has been remained on standby. During this period, the computing 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 the designed RTO/RPO and replication strategy. The storage should be 100% of the capacity of the Primary Data Center site.
- In the event of a site failover or switchover, the DR site has been taken over the active role, and all requests have been routed through that site. Application data and application states have been replicated between data centers so that when an outage occurs, failover to the surviving data center can be accomplished within the specified RTO. This is the period during which the Compute environment for the application shall be equivalent to DC. The installed application instance and the database shall be usable, and the same SLAs as DC shall be provided. The use of this Full Computer DR environment can be for specific periods during the year for DC failure or DR Drills or DC maintenance. The Database and storage shall be of full capacity and the licenses and security shall be for full infrastructure. The bandwidth at the DR shall be scaled to the level of the Data center. Users of the application should be routed seamlessly from the DC site to the DR site. The MSP shall conduct a 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 DRC or vice-versa (regular planned changes), there should not be any data loss.
- The MSP shall clearly define the procedure for announcing DR based on the proposed DR solution. The MSP 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 MSP shall plan all the activities to be carried out during the Disaster Drill and issue a notice to the Department at least two weeks before such drill.
- The MSP should offer a dashboard to monitor the RPO and RTO of each application and database. The MSP should offer switchover and switchback of individual applications instead of the entire system. Any lag in data replication should be visible in the dashboard and alerts of same should be sent to respective authorities.

13.29 Management / Transition-Out Services

- Provide a comprehensive exit management plan, with a focus on sustainability
- Migration of the VMs, data, content, and any other assets to the new environment or on alternate Managed Service Provider's offerings and ensuring successful deployment and running of user Department's solution on the new infrastructure by suitably retrieving all data, scripts, software, virtual machine images, and so forth to enable mirroring or copying to Agency supplied industry-standard media
- Ensure that all the documentation required for smooth transition including configuration documents are kept up to date
- Once the exit process is completed, remove the data, content, and other assets from the cloud environment and destroy the VM, Content, and data of the department.

13.30 Optimal Utilization of Cloud Services and Planning

- To ensure optimal solution design and encourage proper utilization of the assigned computing resources, the MSP in coordination with the department should ensure that the average monthly utilization of RAM, CPU, and storage is not less than 50%.
- If the average monthly utilization is less than 50% in a particular month, the MSP should immediately notify the user Department. The user Department and the MSP/MSP should undertake a joint assessment within 15 days, to analyses the reasons for the utilization being less than 50% and undertake steps to ensure resource utilization of at least 50%.
- If the average monthly utilization of RAM or CPU or storage is less than 50% for 2 successive months, a penalty of 25% of the monthly bill amount (from the next billing cycle) will apply for those months where utilization is below 50%.
- However, if the MSP has proposed a resource optimization plan to bring the average utilization above 50% but such plan has not been approved by the department within the above period of 2 months, the penalty will be waived.

13.31 Helpdesk Support

- The MSP is required to create and maintain a Help Desk / telephonic number and email-based ticketing

system that will resolve problems and answer queries related to DC/DR site.

- The help desk support to users shall be provided on a 24x7x365 basis over telephone, chat, and ticketing system.

13.32 Contract Performance Bank Guarantee (PBG)

- As per GeM

13.33 Right to terminate the tendering Process

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

13.34 Termination of Contract

Department may, without prejudice to any other remedy for breach of contract, by a written notice of default of at least 60 days sent to the selected Bidder, terminate the Contract in whole or in part (provided a cure period of not less than 90 days is given to the selected Bidder to rectify the breach):

- If the selected Bidder fails to deliver any or all quantities of the Service within the time period specified in the Contract, or any extension thereof granted by Department; or
- If the selected Bidder fails to perform any other obligation under the Contract within the specified period of delivery of service or any extension granted thereof; or
- If the selected Bidder, in the judgment of the Department, is found to be engaged in corrupt, fraudulent, collusive, or coercive practices in competing for or in executing the Contract.
- If the selected Bidder commits breach of any condition of the Contract
- If Department terminates the Contract in whole or in part, amount of Performance Guarantee shall be forfeited.

The selected bidder may terminate this Agreement, or any Services, immediately upon written notice to Client if the selected bidder reasonably determine that the selected bidder can no longer provide the Services in accordance with applicable law or professional obligations.

13.35 Financial Proposal

- The proposals shall be valid for a period of six (06) months from the date of opening of the proposals. On completion of the validity period, unless the bidder withdraws his proposal in writing, it will be deemed to be valid until such time that the bidder formally (in writing) withdraws his proposal. In exceptional circumstances, at its discretion, the Department of Agriculture and Farmers' Welfare (DA&FW) may solicit the bidder's consent for an extension of the validity period. The request and the responses thereto shall be made in writing
- In the Financial bid, the Bidder is expected to price/cost for all the items and services as asked. Unless expressly indicated in this tender, bidder shall not include any technical information regarding the services in the financial proposal. Additional information directly relevant to the scope of services provided in the tender may be submitted to accompany the proposal. However, this information will not be considered for evaluation purposes.
- The financial Proposal should not comprise of any direct/ indirect conditions. It is required that all the financial proposals submitted against the tender should be unconditional. If the financial proposal contains conditions the Department of Agriculture and Farmers' Welfare (DA&FW) may consider rejecting such proposals.

13.36 Rights to the Content of the Proposal

- The Department of Agriculture and Farmers' Welfare is not restricted in its rights to use or disclose any or all the information contained in the proposal and can do so without compensation to the bidders. The Department shall not be bound by any language in the proposal indicating the confidentiality of the proposal or any other restriction on its use or disclosure.

13.37 Disqualification of proposal

The proposal is liable to be disqualified in case the bidder fails to meet the bidding requirements as indicated in this

tender:

- Proposal not submitted in accordance with the procedure and formats prescribed in this document or treated as non-conforming proposal
- If a proposal appears to be “canned” presentations of promotional materials that do not follow the format requested in this tender or do not appear to address the requirements of the proposed solution, and any such bidders may also be disqualified
- Proposal is received in incomplete form
- Proposal is received after due date and time at the designated venue
- Proposal is not accompanied by all the requisite documents
- If bidder provides quotation only for a part of the project
- Information submitted for Eligibility and/or in Technical Proposal is found to be misrepresented, incorrect or false, accidentally, unwittingly, or otherwise, at any time during the processing of the contract (no matter at what stage) or during the tenure of the contract including the extension period if any
- Bidder tries to influence the proposal evaluation process by unlawful/ corrupt/ fraudulent means at any point of time during the bid process
- In case any one bidder submits multiple proposals or if common interests are found in two or more bidders, the bidders are likely to be disqualified, unless additional proposals/ bidders are withdrawn upon notice immediately
- Bidder fails to deposit the Performance Security or fails to enter a contract within 60 working days of the date of notice of award of contract or within such extended period, as may be

  specified by Department of Agriculture and Farmers’. Bidders may specifically note that while evaluating the proposals, if it comes to Department of Agriculture and Farmers’ knowledge expressly or implied, that some bidders may have colluded in any manner, whatsoever, or otherwise joined to form an alliance resulting in delaying the processing of proposal then the bidders so involved are liable to be disqualified for this contract as well as fora further period of three years from participation in any of the tenders floated by Department of Agriculture and Farmers’

13.38 Evaluation Committee

- The Department will constitute an Evaluation Committee to evaluate the responses of the Bidders
- The Evaluation Committee shall evaluate the responses to the tender and all supporting documents/ documentary evidence.
- Inability to submit requisite supporting documents/ documentary evidence, within the stipulated time may lead to rejection of the bid.
- The decision of the Evaluation committee in the evaluation of responses to the tender shall be final. No correspondence will be entertained outside the process of evaluation with the Committee.
- The Evaluation Committee may ask for meetings with the Bidders to seek clarifications on their proposals
- The Evaluation Committee reserves the right to reject any or all proposals on the basis of any deviations.
- Each of the responses shall be evaluated as per the criterions and requirements specified in this tender.

14. Annexures

Annexure I: MSP Particulars

#	Description	Details to be filled by MSP
1	Name of the Company	
2	Official address	
3	Phone No. And Fax No.	
4	Corporate Headquarters Address	
5	Details of Company's Registration (Please enclose copy of the company registration document)	
6	Name of the Contact Person	
7	Contact Person Mobile No.	
8	Contact Person E-mail id.	
9	Name of the Bank with full address	
10	Bank Account Number (Enclose an unsigned cheque duly cancelled)	
11	Details of Earnest Money Deposit Name of the Bank Banker's Cheque No. and Date	
12	Registration Number and Year of Registration	
13	GST registration No	
14	TIN No. / Sales Tax No.	
15	Permanent Account Number (PAN)	
17	MeitY Empanelment Validity	
18	Copy of valid certificates	
19	Company's Revenue for last 3 years (Year wise) FY FY 2020-21 FY 2021-22 FY 2022-23	
20	Company's net worth for the last year FY 2020-21 FY 2021-22 FY 2022-23	

Thanking you.

Yours faithfully,

Name…….

Designation…….

Common Seal…….

Annexure II: Letter of Acceptance

<<Department Name>>

<<Department Address>>

<<Pin Code>>

Subject: RFP for Cloud service provider for providing Cloud Hosting and Managed Services Ref: Bid No:

<No> Dated <DD/MM/YYYY>

Dear Sir,

With reference to your Bid Reference No. **<<Reference Number>>**dated **<<date>>**for RFP for Cloud service provider for providing Cloud Hosting and Managed Services, we hereby confirm that we have read the provisions of the bid documents and further confirm to accept all the terms and conditions contained in the bid documents except those against which we have taken deviation in the respective schedules.

Thanking you.

Yours faithfully,

For and on behalf of……

Name…….

Designation…….

Common Seal…….

Annexure III: Qualifying Requirement Data

List of major clients for RFP for Cloud service provider for providing Cloud Hosting and Managed Services shall be uploaded in technical part of the bid in the following prescribed format

Sr. No.	Technology	Client Name and Location	Name of the Project	Project Start Date	Project End Date	Scope / Description of the Project	Contact details (Person name, designation, phone, mobile, email)

Annexure IV: Technical Deviations

Technical Deviations for RFP for Cloud service provider for providing Cloud Hosting and Managed Services for department shall be uploaded through e-procurement in the following prescribed preform.

The following are the Technical deviations and variations from the exceptions to the specifications and documents against Detail Technical Specification in this RFP. These deviations and variations are exhaustive. Except these deviations and variations, the entire work shall be performed as per department's specifications and documents.

Ref: Bid No: **<No> Dated <DD/MM/YYYY>**

#	Section	Clause No.	Page No.	Statement of deviations and variations

Yours faithfully,

For and on behalf of……

Name……

Designation……

Common Seal……

Annexure V: Commercial Deviations

Commercial Deviations for RFP for Cloud service provider for providing Cloud Hosting and Managed Services for department shall be uploaded through e-procurement in the following prescribed preform.

The following are the commercial deviations and variations from the exceptions to the specifications and documents against Detail Technical Specification in this RFP. Except these deviations and variations, the entire work shall be performed as per department's specifications and documents.

Ref: Bid No: <No> Dated <DD/MM/YYYY>

#	Section	Clause No.	Page No.	Statement of deviations and variations

Yours faithfully,

For and on behalf of……

Name……

Designation……

Common Seal……

Annexure VI: Commercial Cover Letter

<<Department Name>>

<<Department Address>>

<<Pin Code>>

Subject: RFP for Cloud service provider for providing Cloud Hosting and Managed Services Ref: Bid No:

<No> Dated <DD/MM/YYYY>

Dear Sir,

We, the undersigned Bidders, having read and examined in detail all the bidding documents in respect of RFP for Cloud service provider for providing Cloud Hosting and Managed Services do hereby propose to provide services as specified in the RFP.

1. Price and Validity

All the prices mentioned in our bid are in accordance with the terms as specified in the bid documents. All the prices and other terms and conditions of this bid are valid for a period of 180 calendar days from the date of opening of the Bids.

We hereby confirm that our bid prices include all taxes. Taxes are quoted separately under relevant sections, as specified in the bid formats.

We have studied the clause relating to Indian Income Tax and hereby declare that if any income tax, surcharge on Income Tax, Professional and any other Corporate Tax in altercated under the law, we shall pay the same.

2. Unit Rates

We have indicated in the relevant schedules enclosed, the unit rates for the purpose of payment as well as for price adjustment in case of any increase to / decrease from the scope of work under the contract.

3. Deviations

We declare that all the services shall be performed strictly in accordance with the bid documents and there are no deviations.

4. Qualifying Data

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

5. Bid Price

We declare that our Bid Price is for the entire scope of the work as specified in the bid document. These prices are indicated in the subsequent sub-sections of this Section.

6. C

ontract Performance Guarantee Bond

We hereby declare that in case the contract is awarded to us, we shall submit the contract Performance Bank Guarantee in the form prescribed in the bid.

We hereby declare that our bid is made in good faith, without collusion or fraud and the information contained in the bid is true and correct to the best of our knowledge and belief.

We understand that our bid is binding on us and that you are not bound to accept a bid you receive. We confirm that no Technical deviations are attached here with this commercial offer.

Yours faithfully,

For and on behalf of……

Name…….

Designation……..

Common Seal…….

Annexure VII: Professional resources details

The following are minimum qualifications and experience for key resources required to implement the cloud solution. The following personnel would be required during the Design, Configuration, Installation and Setup of the Cloud solution. The Project Manager would continue during the post implementation project management phase.

#	Role	Minimum Qualification and Experience
1	Project Manager	· B.E. / B.Tech./MCA or equivalent
		· PMP or equivalent certification
		· 10+ Years of Experience; 5+ years of
		· Experience as Project Manager
		· Present experience of 2+ Years in managing a
		· Cloud- service project
2	Solution Architect	· B.E. / B.Tech. / MCA or equivalent
		· 6+ Years of Experience in Solution Design
3	Cloud Administrator	· B.E. / B.Tech. / MCA or equivalent
		· 8+ Years of Experience in Implementation, Management and Operations
4	System Administrator	· B.E. / B.Tech. / MCA or equivalent
		· 4+ Years of Experience in Implementation, Management and Operations
5	Network Administrator	· B.E. / B.Tech. / MCA or equivalent
		· 4+ Years of Experience in network provisioning, configuration and management
6	Security Administrator	· B.E. / B.Tech. / MCA or equivalent
		· 4+ Years of Experience in Implementation, Management and Operations of security devices and solution

Annexure VIII: CV Format

MSP/MSP has to provide the details on above mentioned resources in the below format.

<table>
<tr><td>1.</td><td>Name of Staff</td><td colspan="5"></td></tr>
<tr><td>2.</td><td>Current Designation in the Organization</td><td colspan="5"></td></tr>
<tr><td>3.</td><td>Proposed Role in the Project</td><td colspan="5"></td></tr>
<tr><td>4.</td><td>Proposed Responsibility in the project</td><td colspan="5"></td></tr>
<tr><td>5.</td><td>Date of Birth</td><td colspan="5"></td></tr>
<tr><td>6.</td><td>Education</td><td colspan="5"></td></tr>
<tr><td>7.</td><td>Summary of Training and Certifications</td><td colspan="5"></td></tr>
<tr><td>8.</td><td>Language Proficiency</td><td>Language</td><td>Read</td><td>Writing</td><td>Speaking</td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr>
<tr><td>9.</td><td>Employment Record (For the total relevant Exp.</td><td>From/To:</td><td colspan="3"></td><td></td></tr>
<tr><td></td><td></td><td>Employer:</td><td colspan="3"></td><td></td></tr>
<tr><td></td><td></td><td>Position Held:</td><td colspan="3"></td><td></td></tr>
<tr><td>10.</td><td>Total No. of Years Working Experience</td><td colspan="5"></td></tr>
<tr><td>11.</td><td>Total No. of Years of Experience for the Role proposed</td><td colspan="5"></td></tr>
<tr><td>12</td><td colspan="6">Highlights of relevant assignment handled and significant accomplishment (use following format for each project)</td></tr>
<tr><td>A</td><td>Name of assignment or Project</td><td colspan="5"></td></tr>
<tr><td></td><td>Years</td><td colspan="5"></td></tr>
<tr><td></td><td>Location</td><td colspan="5"></td></tr>
<tr><td></td><td>Main Project features</td><td colspan="5"></td></tr>
<tr><td></td><td>Positions held</td><td colspan="5"></td></tr>
<tr><td></td><td>Activities performed</td><td colspan="5"></td></tr>
<tr><td></td><td>Positions held:</td><td colspan="5"></td></tr>
<tr><td></td><td>Activities performed:</td><td colspan="5"></td></tr>
</table>

Annexure XI: Format for Non-Disclosure Agreement (NDA)

Non-Disclosure Agreement (NDA) Third

Party Non-Disclosure Agreement

I, _____, on behalf of the _____ (Name of Company), acknowledge that the information received or generated, directly or indirectly, while working with DA&FW on contract is confidential and that the nature of the business of the DA&FW is such that the following conditions are reasonable, and therefore: I warrant and agree as follows: I, or any other personnel employed or engaged by our company, agree not to disclose, directly or indirectly, any information related to the DA&FW. Without restricting the generality of the foregoing, it is agreed that we will not disclose such information consisting of but not necessarily limited to:

- Technical information: Methods, drawings, processes, formulae, compositions, systems, techniques, inventions, computer programs/data/configuration and research projects.
- Business information: Customer lists, project schedules, pricing data, estimates, financial or marketing data.

On conclusion of contract, I, or any other personnel employed or engaged by our company shall return to DA&FW all documents and property of DA&FW, including but not necessarily limited to drawings, blueprints, reports, manuals, computer programs/data/configuration, and all other materials and all copies thereof relating in any way to DA&FW business, or in any way obtained by me during the course of contract. I further agree that I, or any others employed or engaged by our company shall not retain copies, notes or abstracts of the foregoing.

This obligation of confidence shall continue after the conclusion of the contract also. I acknowledge that the aforesaid restrictions are necessary and fundamental to the business of the DA&FW and are reasonable given the nature of the business carried on by the DA&FW. I agree that this agreement shall be governed by and construed in accordance with the laws of country.

I enter into this agreement totally voluntarily, with full knowledge of its meaning, and without duress.
Dated at _____, this _____day of, 20_____.

Signature of the Bidder with stamp

Name
…….…… Designation
…… Date:
……

Annexure XII: Certificate from HR demonstrating its Organization Strength

<<Date>>

<<Department Name>>
<<Department Address>>
<<Pin Code>>

Subject: RFP for Cloud service provider for providing Cloud Hosting and Managed Services Ref: Bid No:

<RFP Reference Number here>Dated <DD/MM/YYYY>

Dear Sir,

This is to certify that our organization has a strength of at least 50 IT Professionals (data centre / networking / system administration / cloud services professional's/cloud security experts) on our payroll as on date of submission of this bid.

At least 10 of these professionals have experience (of minimum 5 years) in maintenance of cloud solution/ DR Management / virtual server administration/system administration, Virtualization, security, database etc.

Yours faithfully,
For and on behalf of…….
Name……..
Designation……
. Common
Seal…….
Date……
HR Signature (with Organization Stamp) HR Name

Annexure XIII: Undertaking by the bidder

<<Date>>

<<Department Name>>
<<Department Address>>
<<Pin Code>>

Subject: RFP for Cloud service provider for providing Cloud Hosting and Managed Services Ref: Bid No:

<RFP Reference Number here>Dated <DD/MM/YYYY>

Dear Sir/ Madam,
We hereby confirm and declare that we,
M/s_____,
have been empaneled by MeitY.
We further certify:

1. We have a running Government Community Cloud (GCC) / Virtual Private Cloud (VPC) service.
2. We are compliant with IT Act 2000 (including 43A) and amendments
3. The proposed Data Centre is in India.
4. Our services are operating in multiple Data Centres across India.
5. Our DC and DR Centres are in two different seismic zones in India
6. All the data that will be acquired and processed through the system will reside in India
7. We have not been blacklisted by any Central / State Government department or public sector undertaking or any regulatory institution nor have been declared ineligible for
corrupt or fraudulent practices as on date of bid submission.
8. We will be the single point of responsibility by owning and providing Cloud services as requested.
9. We will provide the department the flexibility to create resources like Virtual instance, storage and other services of any configuration and not restrict to specific configuration.
10. We have a registered office in Delhi
11. We are not subjected to any legal action for any cause in any legal jurisdiction in the last five years.
12. We have submitted the Earnest Money Deposit to the department

Yours faithfully,
For and on behalf of……
Name……
Designation……
. Common
Seal……
Date……
Enclosure:
Required supporting documents
Additional relevant and required documents if any

Annexure XIV – Format for Power of Attorney / Bidder's Authorization Certificate

Bidder's Authorization Certificate

(To be submitted on the letter head of the Bidder)

To:
Director (Digital Agriculture),
Department of Agriculture and Farmers' Welfare Ministry of
Agriculture and Farmers' Welfare Government of India
026A, Ground Floor, Krishi
Bhawan, Delhi, India –
110001

<Personnel Name>, <Designation> from <Bidder's Name> is hereby authorized to sign relevant documents on behalf of the Proprietorship/ Partnership firm/ Company in dealing with RFP of **<RFP Reference Number here>**dated_____.

He is also authorized to attend meetings and submit technical and commercial information as may be required by you in the course of processing above said RFP.

Yours Sincerely,

Signature of the Bidder with stamp

Name ……..……

Designation

……..…… Date:

……..……

Annexure XV: Financial Bid

7. RFP Ref. No.: **<RFP Reference Number here>**

8. Name of the Bidder: ……

9. The offer with rates for the schedule of requirements of items, as elaborated under, to be submitted. Adhering to the format given below is a Pre-requisite for considering your quotations:

Financial Bid Format

S.No.	Service Name / Type of Service	Configuration/Description of Service	Specifications of required Service	Unit of Measurement of Service*	Proposed	Total Indicative Hours in a Month / Billing Cycle	Offered Price in INR	Total Cost (CSP public pricing =(6x7x8) in INR)	Total offered Cost =(6x7x9) in INR
A. Compute as Managed Service									
1	Non burstable x86 architecture - Production Grade Virtual Machine - on demand	RED HAT Enterprise Linux Including cloud Licenses and native billing for RHEL	VM - 2 vCPU, 4GB RAM	Monthly	1	730			
2			VM - 2 vCPU, 8GB RAM	Monthly	1	730			
3			VM - 2 vCPU, 16GB RAM	Monthly	1	730			
4			VM - 4 vCPU, 8GB RAM	Monthly	2	730			
5			VM - 4 vCPU, 16GB RAM	Monthly	5	730			
6			VM - 4 vCPU, 32GB RAM	Monthly	3	730			
7			VM - 8 vCPU, 32GB RAM	Monthly	2	730			
8			VM - 16 vCPU, 64GB RAM	Monthly	2	730			
9			VM - 32 vCPU, 128GB RAM	Monthly	4	730			
10			VM - 48 vCPU, 192GB RAM	Monthly	2	730			
11			VM - 64 vCPU, 256 GB RAM	Monthly	1	730			
12			VM - 80 vCPU, 320 GB RAM	Monthly	1	730			
13			VM - 96 vCPU, 384 GB RAM	Monthly	1	730			
14			VM - 128 vCPU, 512 GB RAM	Monthly	1	730			

15			VM - 224 vCPU, 224 GB RAM	Monthly	1	730			
16		Open-Source Linux - Debian, CentOS, Ubuntu	VM - 2 vCPU, 4GB RAM	Monthly	30	730			
17			VM - 2 vCPU, 8GB RAM	Monthly	25	730			
18			VM - 2 vCPU, 16GB RAM	Monthly	20	730			
19			VM - 4 vCPU, 8GB RAM	Monthly	40	730			
20			VM - 4 vCPU, 16GB RAM	Monthly	150	730			
21			VM - 4 vCPU, 32GB RAM	Monthly	5	730			
22			VM - 8 vCPU, 32GB RAM	Monthly	75	730			
23			VM - 16 vCPU, 64GB RAM	Monthly	40	730			
24			VM - 32 vCPU, 128GB RAM	Monthly	50	730			
25			VM - 48 vCPU, 192GB RAM	Monthly	10	730			
26			VM - 64 vCPU, 256 GB RAM	Monthly	30	730			
27			VM - 80 vCPU, 320 GB RAM	Monthly	10	730			
28			VM - 96 vCPU, 384 GB RAM	Monthly	10	730			
29			VM - 128 vCPU, 512 GB RAM	Monthly	40	730			
30			VM - 224 vCPU, 224 GB RAM	Monthly	20	730			
31		Windows O/S with Cloud Based O/S Licenses & native billing	VM - 2 vCPU, 8GB RAM	Monthly	25	730			
32			VM - 4 vCPU, 16GB RAM	Monthly	135	730			
33			VM - 8 vCPU, 32GB RAM	Monthly	200	730			
34			VM - 16 vCPU, 64GB RAM	Monthly	30	730			
35			VM - 32 vCPU, 128GB RAM	Monthly	5	730			

36			VM - 48 vCPU, 192GB RAM	Monthly	5	730			
37			VM - 64 vCPU, 256 GB RAM	Monthly	5	730			
38			VM - 80 vCPU, 320 GB RAM	Monthly	5	730			
39			VM - 96 vCPU, 384 GB RAM	Monthly	5	730			
40			VM - 128 vCPU, 512 GB RAM	Monthly	10	730			
B. Storage as a Managed Service - Object, File and Block Storage									
1	Object Storage - Hot Tier	Managed Object Storage	Fully Managed Redundant Object Storage - 100% Hot Tier	TB per month	1200	Monthly			
2	Archive Storage with millisecon ds restore tier	Managed Archival Storage - Restored quickly in millisecond s	Fully Managed Geo Redundant Archival/ Cold Tier with instant restore time	TB per month	1500	Monthly			
3	Cloud Native Enterprise-grade network file system (NFS)	Enterprise-grade network file system (NFS)	TB of provisioned capacity	TB Per Month	30	Monthly			
4	Managed Storage-SSD	Managed SSD Storage for Mission Critical Web, Apps and Databases	Single SSD redundant volume with 6,000 Provisioned IOPS/TB or 6 IOPS /GB from Storage tier which support 64 TB per volume with Sub-millisecond latency performance .	TB per month	500	Monthly			

5			Single SSD redundant volume with 30,000 Provisioned IOPS/TB or 30 IOPS /GB from Storage tier which support 64 TB per volume with Sub-millisecond latency performance .	TB per month	600	Monthly			
C. Managed DB - Native Managed services by CSP									
1	CSP Native Managed Database services (Non burstable x86 Intel architecture - Production Grade)	PostgreSQL /MySQL as a service with following features: 1) Automated backups and point-in-time recovery 2) Automatic Storage Increase 3) Support Multi AZ architecture with Sync Replication 4) Should support horizontal scaling by adding/removing read replicas Bidder must Quote the	2 vCPU 8 GB RAM	Monthly	1	730			
2			4 vCPU 16 GB RAM	Monthly	1	730			
3			8 vCPU 32 GB RAM	Monthly	1	730			
4			16 vCPU 64 GB RAM	Monthly	1	730			
5			32 vCPU 128 GB RAM	Monthly	1	730			
6			48 vCPU 192 GB RAM	Monthly	1	730			
7			64 vCPU 256 GB RAM	Monthly	1	730			
8			96 vCPU 384 GB RAM	Monthly	1	730			

		CSP Managed DB Service with HA architecture & Configuration (e.g. Active/Standby) for the Pricing							
9		MS SQL Server 2017 / 2019 / 2022 Enterprise as a service with following features: 1) Automated backups and point-in-time recovery 2) Automatic Storage Increase 3) Support Multi AZ architecture with Sync Replication 4) Should support horizontal scaling by adding/removing read replicas Bidder must Quote the CSP Managed DB Service with HA architecture &	2 vCPU 8 GB RAM	Monthly	1	730			
10			4 vCPU 16 GB RAM	Monthly	1	730			
11			8 vCPU 32 GB RAM	Monthly	1	730			
12			16 vCPU 64 GB RAM	Monthly	1	730			
13			32 vCPU 128 GB RAM	Monthly	1	730			
14			48 vCPU 192 GB RAM	Monthly	1	730			
15			64 vCPU 256 GB RAM	Monthly	1	730			
16			96 vCPU 384 GB RAM	Monthly	1	730			

		Configuration (e.g. Active/Standby) for the Pricing							
17		MS SQL Server 2017 / 2019 / 2022 Standard as a service with following features: 1) Automated backups and point-in-time recovery 2) Automatic Storage Increase 3) Support Multi AZ architecture with Sync Replication 4) Should support horizontal scaling by adding/removing read replicas Bidder must Quote the CSP Managed DB Service with HA architecture & Configuration (e.g. Active/Standby) for the Pricing	2 vCPU 8 GB RAM	Monthly	1	730			
						730			
						730			
18			4 vCPU 16 GB RAM	Monthly	1	730			
19			8 vCPU 32 GB RAM	Monthly	1	730			
20			16 vCPU 64 GB RAM	Monthly	1	730			
21			32 vCPU 96 GB RAM	Monthly	1	730			
22			48 vCPU 128 GB RAM	Monthly	1	730			

23	CSP Native Redis Cluster as Service - Production Grade supporting Sharding	Managed Redis as a Service with: - Should support the Managed Cache database service - Supports partitions/ shards and read replicas - Must be compatible with open-source Redis data store - Inbuilt capability to auto-scale shards and read replicas - Persists data stored in Redis Cache - Shards data across Redis nodes	130 GB Enterprise Grade Redis with Sharding support	Monthly	15	730			
24	Production Grade CSP Native Managed Non-Relational Database(NoSQL) as Managed Services	Scalable NoSQL DB as Managed Service 1) Automated replication /Automatic failover to another Zone and region 2) Automated Backup 3) Multi -	Storage (GB) - 500 , Number of writes / Second: 1000 , Number of reads / Second: 2000, Backup - 30 days	Monthly	15	730			

		AZs HA architecture							
D: Other CSP Managed /additional services/Network /Back up / Security									
1	CSP native Container Registry	Container Registry allows you to build, store, and manage container images and artifacts in a private registry for all types of container	Container Registry - 100GB/Month	100GB/Month	2	Monthly			
2	Managed Kubernetes (Production Grade, SLA Backed)	Container Orchestration service to deploy, scale and manage container-based applications in a cluster environment. Should support service mesh for observability, network and security.	Fully Automated highly available & scalable managed Kubernetes Cluster / Month	Monthly	2	730			
3	Cloud Management and Monitoring	Monitoring, Logging & Alerts for cloud resources	Monitoring and observability service, with data and actionable insights to monitor applications, respond to system-wide performance changes, optimize resource utilization, and a unified view of	Logs of 1000 GB per month.	1	Monthly			

			operational health.						
4	Site to Site VPN - CSP Managed Service	Fully managed Site to Site VPN	VPN Connectivity as Site-to-Site VPN with upto 1.25 Gbps bandwidth per VPN tunnel	Monthly	50	Monthly			
5	DevOps and Application Monitoring	CI/CD Pipeline (Should provide a fully managed build service that supports continuous integration and deployment.)	Continuous Integration and Code Deployment Pipelines with min 5 users	Per month	10	Monthly			
6			Build Minutes [Min 4 vCPU and 8GB RAM build server]	100hrs/Per month	10	Monthly			
7	CSP Natively Managed Application Load balancer (L7)	Managed service to provide automated traffic distribution from one entry point to multiple back ends over layer 7	Should provide an Application Gateway as an external facing layer 7 load balancer which supports SSL termination, cookie-based session affinity and round robin for load-balancing traffic. Load Balancers with data being	Per month	20	Monthly			

			processed up to 1TB/month						
Added	SSL Certificate				200	Monthly			
8	CSP Natively Managed TCP Load balancer(L 3/L4)	Managed service to handle high volumes of TCP traffic	Load Balancers with data being processed up to 1TB/month	Per month	50	Monthly			
9	NAT Gateway	Managed NAT Gateway for outbound Internet Access for Private Instances	100GB of data Processed/M onth	Per month	10	Monthly			
10	Backup as Service	Full managed backup service	Back up key data stores, such as volumes, databases, and file systems, across cloud resources, Policy based Centralize & automated data protection management and Backup role-based access control , Backup activity monitoring	per TB / per month	50	Monthly			
11	Domain Name System (DNS)	Managed DNS service that supports all common DNS record types with following features:	Per Domain Name per month	With 5 Hosted Zone and 50 Million Queries	10	Monthly			

		- Weighted round robin (WRR) routing policy - Geofenced routing policy - Failover routing policy							
12	Data transfer /Egress over the Internet	Data Transfer Egress from Compute , database, Object Storage etc. over the Internet	Data transfer out per month	Per GB	10000	Monthly			
13	Direct Connect / Interconnect to connect MPLS/ Lease Line to cloud	Interconnect Port with capacity of 1 Gbps	Link termination inside a VPC	Per Port	1				
14	Messaging services	Should provide a managed message queueing service for communicating between decoupled application components	Standard queue requests and FIFO queue requests in millions /1GB Volume with number of Subscriptions per Month	Monthly	1	Monthly			
15	Public IP	Public IP for VMs and LBs	Per Public IP	Monthly	150	Monthly			
16	CSP Native SIEM Enterprise solution	Raw log information for building detection capability, improving	Ingestion in GB	Monthly Per GB	2500	Monthly			

		risk analytics, and extending logs for investigating.							
17	Cloud Posture Management	Identify cloud misconfigurations, software vulnerabilities, and compliance violations and get visibility of cloud assets and resources on single Dashboard	Centralised Threats and Vulnerabilities reporting on Single Dashboard	Events or cloud operation analysed/month	5000	Event/cloud operation per month			
18	Managed DdoS Protection and WAF	Web Application Firewall CSP Natively Managed	Managed service to protect Layer7 application attacks like SQL Injection with 10 WAF Rules	1 Million Request/ Month.	4	Monthly			
19	Network Firewall - Cloud Native NGFW	CSP Native Managed Network Firewall - IPDS NGFW with Transport Layer Security (TLS) interception and decryption	Managed Network Firewall with intrusion detection / prevention system. Each firewall endpoint will process 50 Terabyte of traffic /50 TB data processed per month , the Billing will be based on the actual consumption	Monthly	4	Monthly			
E : CSP Native Content Delivery Network (CDN)									

1	Managed CSP Native Content Delivery Network (CDN)	TB egress / data transfer out over CDN	CDN service to be used to securely deliver audio, video, images, data, application, etc., quickly by using the servers closest to each user. CDN to reduce load time and saves bandwidth.	TB per Month	4	Monthly			
F : CSP Native AI/ML & Data Warehouse Platform									
1	ML Notebook	Fully managed CSP native Notebook IDE - Fully Managed & collaborative Jupyter Notebook - to perform all ML development steps (Prepare, build, Train & Deploy) from a single Web based visual interface.	Node Size 16 vCPU 64 GB RAM	Monthly	2	730			
2	ML Training	Fully managed CSP native Training Jobs Service: GPU-powered instances for running training jobs. One Node -	Node Size: 24vCPU, 96 GB RAM with 2 GPUs / training job per month/730hrs	Monthly	2	730			

		(24vCPU, 96GB of memory, 2 Nos of GPUs that supports TensorFlow, PyTorch, XgBoost ML-API for training Models and network performance of 32 Gbps)- Latest GPU with launch date not earlier than 2023							
3	ML Inference	Real Time Inference	Node Size 16 vCPU 64 GB RAM	Monthly	2	730			
4	Fully Managed Data Warehouse	Full managed Datawarehouse with - Cloud-based enterprise data warehouse (EDW) to run complex queries across petabytes of data.	Data Warehouse Platform: a. Cloud-based enterprise Data warehouse - each unit/node having minimum configuration of 4 vCPU & 32 GB RAM, for running complex Queries(Approximate 100 Queries in Month with each query scanning of minimum of 100GB of data with 4 dedicated	Monthly	1	730			
						730			

			nodes/units for Number of units in estimated units with 100% utilization of dedicated nodes; Or b. Fully Managed Cloud-based Serverless data warehouse - should run complex queries (Approximate 100 Queries in Month with each query scanning minimum of 100GB of data for Number of units in estimated units) Pls Note: Bidder to quote only one (either a or b) option, which must support HA cluster deployment & Data Governance features including Row level Security , Data Masking, and cluster encryption using Customer						

			Managed Key						
5	Managed ETL as a Service	Managed ETL Service: - Serverless service to process and transfer data between different compute and storage services data sources at specified intervals, create, schedule, orchestrate and manage data pipelines	4vCPU and 16GB	Monthly	1	730			
6	Data Visualization /BI Service	Fully Managed Serverless service with - Auto-scalable - Data visualization service for telemetry data and operational metrics	Data Visualization Service	Monthly	1	730			
G : Generative AI As Service									
1	GenAI - Multimodal models	Multimodal Managed large	Image Input/image	million/Month	1	Monthly			

2		model API for Image, Video, Text & Audio	Video Input/second	1000000	1	Monthly			
3			Text Input & output - Token	million/Month	1	Monthly			
4			Audio Input/second	1000000	1	Monthly			
5	Translation	Text Translation - CHAR	Text Translation (characters) in Million	million/Month	1	Monthly			
6		Text Translation - Documents	Document Translation (pages)	Number of Pages	400	Monthly			
7		Speech to Text	Speech-to-Text in minutes	minutes/Month	1000	Monthly			
8	Enterprise Chat bot	Peak requests per day - Text	Number of requests per month	Request/Month	400000	Monthly			
9		Peak requests per day- Voice	Number of seconds per month	Sec/Month	50000	Monthly			
10		Peak requests per day- Data Index	Amount of GB indexed per month	DB/Month	50	Monthly			
11		Search LLM	LLM based Search	Request/Month	400000	Monthly			
H: MS-SQL Licenses Provided by CSP									
1	MS SQL 2017 / 2019 / 2022 Cloud based Image Licenses	Pre-configured virtual machine image with Microsoft SQL Server already installed on a Windows Server operating system. The bidder must Quote SQL core based licenses	4 vCPU, 32 GB RAM	Enterprise	2	730			
2			16 vCPU, 128 GB RAM	Enterprise	2	730			
3			32 vCPU, 512 GB RAM	Enterprise	2	730			
4			48 vCPU, 384 GB RAM	Enterprise	2	730			
5			48 vCPU, 512 GB RAM	Enterprise	3	730			

6		offered by CSP as pre-configured image with Windows OS & SQL server	64 vCPU, 512 GB RAM	Enterprise	2	730			
7			128 vCPU, 512 GB RAM	Enterprise	15	730			
8			2 vCPU, 4 GB RAM	standard	15	730			
9			4 vCPU, 16 GB RAM	standard	2	730			
10			2 vCPU, 8 GB RAM	web	3	730			
11			2 vCPU, 16 GB RAM	web	1	730			
12			4 vCPU, 4 GB RAM	web	2	730			
13			4 vCPU, 8 GB RAM	web	3	730			
14			4 vCPU, 16 GB RAM	web	40	730			
15			8 vCPU, 16 GB RAM	web	3	730			
16			8 vCPU, 32 GB RAM	web	2	730			
17			8 vCPU, 64 GB RAM	web	1	730			
18			16 vCPU, 16 GB RAM	web	1	730			
19			16 vCPU, 32 GB RAM	web	1	730			
20			16 vCPU, 64 GB RAM	web	3	730			
21			32 vCPU, 32 GB RAM	web	1	730			
I: One-time migration cost including 2 Month of trial operations					1				

Annexure XV: Financial Bid

10. RFP Ref. No.: **<RFP Reference Number here>**

11. Name of the Bidder: ……

12. The offer with rates for the schedule of requirements of items, as elaborated under, to be submitted. Adhering to the format given below is a Pre-requisite for considering your quotations:

Financial Bid Format

Sr. no	Category		Total Cost (CSP public pricing =(6x7x8) in INR)	Total offered Cost =(6x7x9) in INR
1	Category A	Compute as Managed Service - On Demand	-	-
2	Category B	Storage as a Managed Service - Object, File	-	-

		and Block Storage		
3	Category C	CSP Managed DB - Native Managed services by CSP	-	-
4	Category D	Other CSP Managed /additional services/Network /Back up / Security	-	-
5	Category E	Content Delivery Network (CDN)	-	-
6	Category F	AI/ML & Data Warehouse Platform	-	-
7	Category G	Generative AI as Service	-	-
8	Category H	CSP MS-SQL Licenses	-	-
9	Category Support	On-Time Migration, Bidder 24x7 Support, CSP Support & Cloud Dedicated Resources	-	-
		GRAND TOTAL	**-**	**-**

PIs Note: The Discount provided as part of this bid document will be used to procure any additional cloud service or configuration of service offered by CSP in future. If additional services do not belong to any category e.g. A, B ,C and D (excluding Category -E as CDN), the discount will be calculated based on overall category " **aggregated Avg. discount %"** (excluding Category -E as CDN)

Note:

- Item Unit Cost should be without Tax (GST)
- Kindly do not enter DC + DR rates as only unit price is requested
- * Unit of Measurement of Service for Compute resources - Monthly is considered as a unit of 730 hours, and year will be 730 * 12
- Unit of Measurement of Service is in TB/Month for Data transfer/Storage resources and may vary for different resources as mentioned in the table above
- Wherever Percent is asked it should be rounded off to 2nd decimal place, avoid making mistakes as 0.19% will be considered as 0.19 and 19% will be considered as 19.00 in total calculation
- Bidder should provide an exhaustive list of services with specifications where 12-month trial can be availed and list of services which are usually provided Free of Cost by the Cloud Service Provider
- All the unit price mentioned for an item should be at discounted rate than the public listed price
- The bidder should provide the calculator link for items quoted in BoM for All Cloud Services mentioned in " Indicative Technical Bill of Material" . The Indicative Technical Bill of Material" and " Financial Bid Format" must be same with CSP list pricing, required Storage IOPS, Database sizing, In case there's any discrepancy with respect to change in the CSP list pricing among the 2 tables , the bid will be disqualified.
- The discount percentage, final pricing of cloud services, and other one-time/ monthly services, must be submitted with financial bid ONLY. Please read the financial bid structure for more details. Submission of any pricing except public list prices of cloud services in the technical bid may lead to rejection of the bid.
- All the prices must be excluding any free tier benefits. For example, in case a service provides 1 TB data transfer out per month free of charge, and charges for additional incremental per TB data transfer over and above that, the bidder must quote prices of the item applicable over and above free tier benefit. If the bidder quotes price for any item as Zero ('0'), it will be treated as a zero cost item throughout the contract period
- Bidders shall note that this RFP is being floated to discover the envisaged cloud services and rates thereof for quantities estimated basis current assessments. Actual consumption and quantities of cloud services may vary from the BoQ. And payments shall be made on actual items/services and quantities consumed during the contract period.

I/we hereby confirm that to the best of our knowledge and belief:

1) The rate quoted will be reasonable and valid for the period of 3 years from the date of opening of financial Bid. The period can be extended with mutual agreement.
2) RFP rates are at par with the prevailing market rates, and not more than the price usually charged for the same nature/class or description from any other, either foreign or as well as Government purchaser.
3) In respect of indigenous items/services for which there is a controlled price fixed by law, the price quoted is not higher than the controlled price.
4) Services/Products/Goods supplied, will be of requisite specification and quality.

Note:

- The Bidders are advised to quote rate in absolute Indian Rupees.
- The rate quoted will be reasonable and valid for the period of contract from the date of opening of financial Bid. The period can be extended with mutual agreement.
- No condition will be entertained, and conditional RFP will be liable to be rejected.

Signature of the Bidder with stamp
Name: …….
Designation: …….
Date: ……

Annexure XVII: Summary of TRS and FRS (To be submitted on company letter head)

#	Requirement category	Yes	No
1	Cloud Portal		
2	General Cloud Requirement		
3	Cloud Portal Service Provisioning		
4	Web Application Firewall		
5	CSP Native SIEM Solution		
6	Criteria for CSP (Cloud Service Provider) with Product/Service Public Link		
7	Cloud Native CDN (Content Delivery Network) compliances		
8	Technical Evaluation criteria - with Product Public Links		
9	Indicative Bill of Materials with Public Price on Product Page/Calculator links		
Total			

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