Request for Proposal (RFP)
for
Provisional Accreditation of
Cloud Service Offerings of Private Service Providers (CSPs)

Department of Electronics and Information Technology
Electronics Niketan, 6, CGO Complex
New Delhi-110 003

30th December 2015

This Page is Intentionally Left Blank

Contents

1. Background

MeghRaj Policy of Government of India

Cloud Computing Services provide the new model of offering services (including IaaS, PaaS and SaaS) to the users at fast pace which is also cost effective. In order to utilize and harness the benefits of Cloud Computing, Government of India has embarked upon a very ambitious and important initiative – "GI Cloud" which has been coined as **MeghRaj**. The focus of this initiative is to evolve a strategy and implement various components including governance mechanism to ensure proliferation of Cloud in government.

DeitY has announced MeghRaj Policy to provide strategic direction for adoption of cloud services by the Government (http://deity.gov.in/content/gi-cloud-initiative-meghraj). The aim of the cloud policy is to realize a comprehensive vision of a government private cloud environment available for use by central and state government line departments, districts and municipalities to accelerate their ICT-enabled service improvements. MeghRaj policy of DeitY states that "Government departments at the Centre and States to first evaluate the option of using the GI Cloud for implementation of all new projects funded by the government. Existing applications, services and projects may be evaluated to assess whether they should migrate to the GI Cloud."

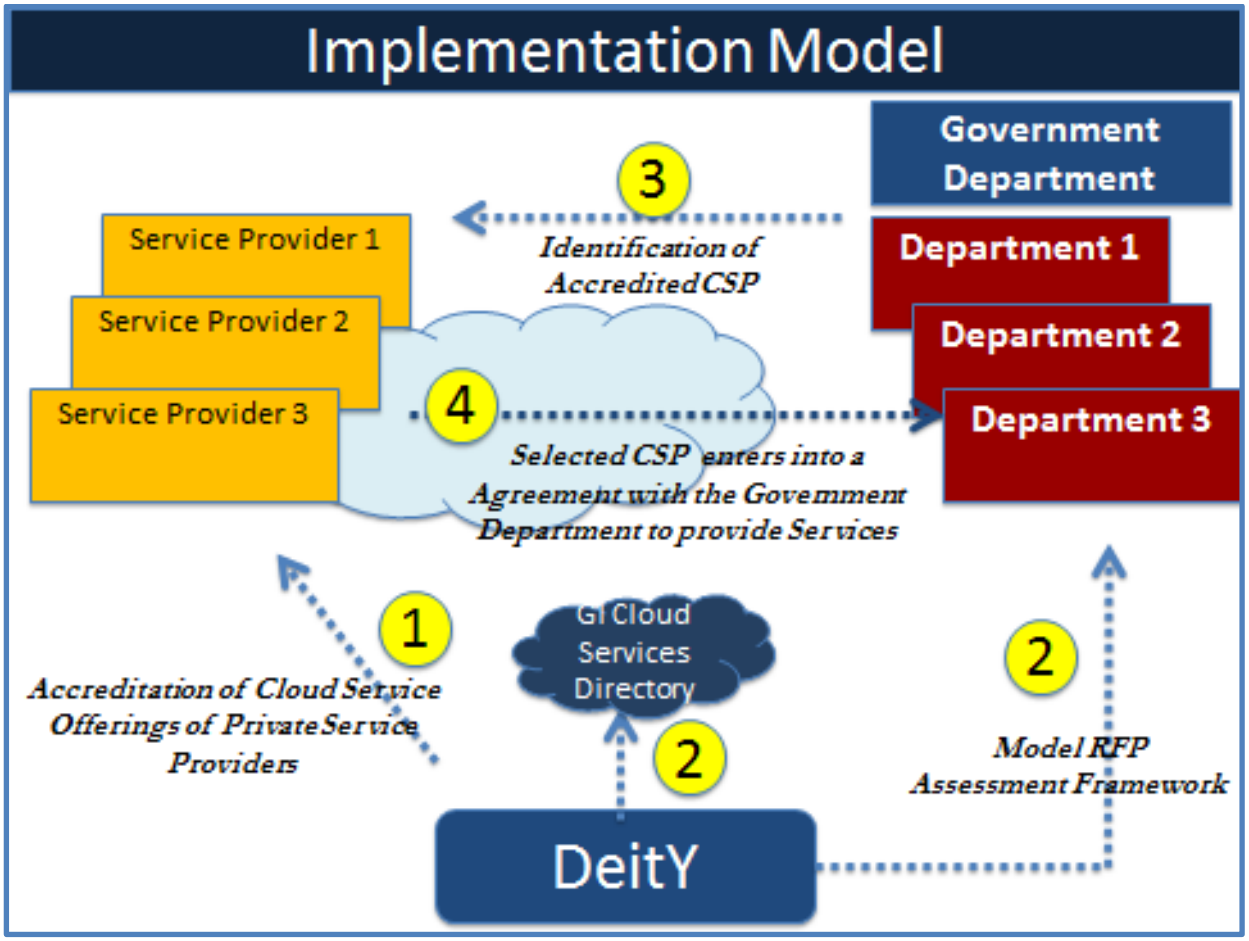
As per the MeghRaj policy, it is proposed to setup GI Cloud, Government of India's cloud computing environment. GI Cloud will be a set of discrete cloud computing environments spread across multiple locations, built on existing or new (augmented) infrastructure, following a set of common protocols, guidelines and standards issued by the Government of India.

National and State Clouds

Government of India has setup National Cloud (under NIC) and also has initiated setup of State Clouds, cloud computing environments at the State Level – building on or augmentation of the infrastructure investments already made.

Accreditation – Cloud Service Offerings of Private Service Providers

At the same time, taking demand into consideration, DeitY proposes Accreditation of the cloud service offerings of Private Service Providers that the end-user departments can leverage in addition to the National Cloud services offered by NIC for their e-governance solutions. The cloud services, offered under National Cloud as well as the Accredited cloud service offerings of the Private Service providers, will be published through a GI Cloud Services Directory for use by government departments or agencies at the Centre and States.



In order to be accredited by DeitY and be part of the GI Cloud Services Directory, the cloud service offerings will require certification of compliance to a common set of standards and guidelines on the security, interoperability, data portability, SLAs and contractual terms & conditions. It is expected that the audit of cloud services to verify the compliance will be carried out by the cloud auditors, who are in turn accredited by DeitY.

DeitY has initiated the process of identification of the relevant Standards, develop the necessary specifications, frameworks and guidelines with the help of a Cloud Management Office (CMO). Given the complexity of the various underlying issues and multitude of work-

items to be covered by CMO, the guidelines and accreditation of offerings of private CSPs is expected only 12 – 18 months from the date of on-boarding of CMO.

Provisional Accreditation

While Cloud Management Office (CMO) will proceed as planned, the current objective is to fast-track the accreditation processes for at least a few of the cloud service offerings from the private providers. Since all the critical areas that need to be addressed for leveraging cloud services from a private service provider may not be possible in the short time span, the current accreditation is referred to as “Provisional Accreditation” with a provision to get fully accredited once the full-fledged guidelines & standards are published by DeitY. The provisionally accredited cloud service providers will have the option to comply with the full-fledged guidelines / standards to get the full accreditation as and when the new guidelines / standards are published by DeitY.

2. Purpose of the RFP

The primary purpose of this RFP is to enable DeitY to provisionally accredit the below cloud service offerings of Private Service Providers (CSPs) for an initial period of two years. This will be an open accreditation process (accreditation window to be opened at defined intervals) to allow for new entrants to accredit their cloud service offerings as well as accreditation of additional cloud service offerings of the existing cloud service providers. The provisionally accredited cloud services offered by private Service providers, will be published through a GI Cloud Services Directory for use by government departments or agencies at the Centre and States.

The details of the accreditation, responsibilities of the cloud service providers, evaluation process are outlined in the sections below.

DeitY invites proposals from the private service providers offering cloud services (hereinafter referred to as "Bidders") for provisional accreditation of the one of more of the below cloud service offerings for a combination of the Deployment Models (Public Cloud, Virtual Private Cloud and Government Community Cloud):

1. Infrastructure as a Service (IaaS)
2. Platform as a Service (PaaS)
3. Disaster Recovery as a Service (DRaaS)
4. Dev / Test Environment as a Service (DevOps)
5. Virtual Desktops as a Service (VDaaS)

The Government Departments will select the appropriate cloud service offerings based on the risk & security profile of their applications / data / services.

The RFP is not an offer by DeitY but an invitation to receive proposals from eligible and interested Bidders in respect of the above-mentioned requirement. The RFP does not commit DeitY to enter into a binding agreement in respect of the project with the potential bidders. Potential bidders are henceforth referred to as "Bidders" in this document.

3. RFP Issuing Authority

This RFP is issued by the Department of Electronics and Information Technology (DeitY) to the Bidders and is intended to provisionally accredit one or more cloud service offerings of Private Service Providers (CSP). DeitY's decision with regard to the accreditation through this RFP shall be final and DeitY reserves the right to reject any or all the bids without assigning any reason.

S. No.	Item	Description
1	**Project Title**	**Provisional Accreditation of Cloud Service Offerings of Private Service Providers (CSP)**
2	**Project Initiator and Issuer Details**	
	Department	**Department of Electronics and Information Technology (DeitY)**
	Contact Person	Kshitij Kushagra Scientist D/Joint Director Department of Electronics and Information Technology Electronics Niketan , 6, CGO Complex New Delhi-110 003 Tel: +91-11- 24301423
	Contact Person (Alternate)	Uma Chauhan Scientist F/ Director Department of Electronics and Information Technology Electronics Niketan , 6, CGO Complex New Delhi-110 003 Tel: +91-11-24364711
	Email Address for all Bid Correspondence	**kshitij.kushagra@deity.gov.in**
	Address for the purpose of Bid Submission	**Kshitij Kushagra** **Scientist D/Joint Director** **Room No. – 4052, 4th Floor** **Department of Electronics and Information Technology,** **Electronics Niketan , 6, CGO Complex** **New Delhi-110 003**
	DeitY Website Central Public Procurement Website	http://deity.gov.in/ http://eprocure.gov.in

4. Tentative Calendar of Events

The following table enlists important milestones and timelines for completion of bidding activities:

S. No	Milestone	Date and time
1	Release of Request For Proposal (RFP)	30th December 2015
2	Last date for submission of written questions by bidders	8th January 2016
3	Pre- Bid Conference	12th January 2016; 15:00 hours
4	Date of Issue of Clarifications	14th January 2016
5	Last date for Submission of bids	29th January 2016; 16:00 hours
6	Opening of Pre-Qualification Bids	29th January 2016; 16:30 hours

Venue for Pre-Bid Conference:

Conference Hall # 1007, Department of Electronics and Information Technology,
Electronics Niketan, 6, CGO Complex,
New Delhi-110 003

5. Compliance Requirements

The cloud service offerings of the private service provider (CSP) must comply with the below mandatory requirements to qualify for getting provisionally accredited.

In the scenario where one or a combination of IaaS, PaaS, DevOps and VDaaS cloud service offerings of the private service provider (CSP) are proposed to be accredited, the CSP also has the option to provide one or a combination of the managed services.

The requirements are divided into categories as follows:

Nature of the Requirement	IaaS	PaaS	DRaaS	DevOps	VDaaS
i. Deployment Model Specific Requirements	Mandatory for All Services				
ii. General Requirements	Mandatory for All Services				
iii. Service Management and Provisioning Requirements	Mandatory for All Services				
iv. User/Admin Portal Requirements	Mandatory for All Services				
v. Integration Requirements	Mandatory for All Services				
vi. LAN / WAN Requirements	Mandatory for All Services				
vii. Data Center Facilities Requirements	Mandatory for All Services				
viii. Cloud Storage Service Requirements	Mandatory for All Services				
ix. Virtual Machines Requirements	Mandatory for All Services				
x. Disaster Recovery & Business Continuity Requirements	**Mandatory for offering DRaaS** **Optional for other services**				
xi. Security Requirements	Mandatory for All Services				
xii. Legal Compliance Requirements	Mandatory for All Services				
xiii. Management Reporting Requirements	Mandatory for All Services				

xiv. Exit Management / Transition Requirements	Mandatory for All Services
xv. Managed Services Requirements	**Not Applicable for DRaaS** **Optional for All Services**

The compliance must be maintained on an on-going basis in order to retain the provisional accreditation status. The mandatory requirements for the respective services in this section also form the minimum scope of work of the provisionally accredited cloud service providers when offering cloud services to the Government.

DeitY has initiated the process of identification of the Standards, develop the necessary specifications, frameworks and guidelines with the help of a Cloud Management Office (CMO). The provisionally accredited cloud service offerings will have the option to comply with the full-fledged guidelines & standards as and when the such guidelines / standards are published by DeitY to get the full accreditation within the timeframe given by DeitY. CSP is responsible for all costs associated with implementing, assessing, documenting and maintaining the accreditation.

In case of delay in publishing full-fledged guidelines / standards by CMO or identification of any critical gaps or deemed as required by DeitY during the period of provisional accreditation, additional guidelines / standards may be published by DeitY from time to time that will be applicable for the Provisionally Accredited Cloud Service Offerings. Provisionally accredited cloud service offerings must comply with the additional guidelines / standards (applicable for the Provisionally Accredited Cloud Service Offerings) as and when such guidelines / standards are published by DeitY at no additional cost to retain the provisional accreditation status. Private Service Providers will be given sufficient time and notice period to comply to the additional guidelines / standards. Any downtime during such upgrades will not be factored for SLA calculations.

5.1. Deployment Model Specific Requirements

Requirement	Public Cloud	Virtual Private Cloud	Government Community Cloud
1. Shall provide services on a Public Cloud.	Y	Y	N
2. Shall provide services on a logical dedicated cloud (herein after referred to as **Government Virtual Private Cloud**) at the Data Center.	N	Y	N
3. Shall be hosted and provided services on a dedicated cloud (herein after referred to as **Government Community Cloud**) at the Data Center.	N	N	Y
4. Government Virtual Private Cloud environment will only offer cloud services for Departments / Ministries / Agencies / Offices of Government of India or States or UTs or PSUs or Nationalized Banks within India (herein after referred to as **Government Department**).	N	Y	N
5. Government Community Cloud will only offer cloud services for Departments / Ministries / Agencies / Offices of Government of India or States or UTs or PSUs or Nationalized Banks within India (herein after referred to as **Government Department**).	N	N	Y
6. The infrastructure elements including server, storage (including backup storage) and network of the Government Virtual Private Cloud should provide strong tenant isolation, provide granular identity and access management capability and encryption and be logically separate from the public and other cloud offerings of the cloud service provider.	N	Y	N

There should be logical separation (of space, servers, storage, network infrastructure and networks) to protect data, applications and servers and provide robust virtual isolation for the Government Virtual Private Cloud.			
7. The infrastructure elements including physical server, physical storage (including backup storage) and network infrastructure of the Government Community Cloud should be dedicated to the Government Department solutions and be physically separate from the public and other cloud offerings of the Cloud Service Provider. There should be physical and logical separation (of space, servers, storage, network infrastructure and networks) to protect data, applications and servers. However, the dedicated infrastructure elements can be shared by the Government Departments.	N	N	Y
8. The space allocated for the dedicated infrastructure should be clearly demarcated and identified as hosting Government Department's Projects. The demarcated and identified area shall not host any components other than those of Government Departments Projects.	N	N	Y
9. The entire N/W Path for each of the hosted government applications shall be separate (logical separation & isolation) from the other clients (including other government departments) and should be dedicated for the respective Government Department.	N	Y	Y
10. Implement a firewall policy that allows the	N	Y	Y

Government Department to administer it remotely, or shall administer a firewall policy in accordance with the Government Department's direction, allowing the Department to have read-only access to inspect the firewall configuration.			
11. The cloud service offering shall support Network and security with virtual firewall and virtual load balancer integration for auto-scale functions.	Y	Y	N
12. The cloud service offering shall support Network and security with dedicated virtual firewall and virtual load balancer integration for auto-scale functions.	N	Y	N
13. The cloud service offering shall support Network and security with dedicated firewall and load balancer integration for auto-scale functions. However, the dedicated infrastructure elements can be shared by the Government Departments.	N	N	Y
14. Must have Separate VLAN provision with dedicated virtual firewall between the VLANs and for each and every client on the Government Virtual Private Cloud.	N	Y	N
15. Must have Separate VLAN provision with dedicated firewall between the VLANs and for each and every client on the dedicated Government Community Cloud.	N	N	Y
16. The management consoles should only show the data relevant for the Government Department.	Y	Y	Y
17. The management consoles for the dedicated Government Community Cloud should only	N	N	Y

show the data for the dedicated Government Community Cloud and in the same manner, the monitoring data of the dedicated Government Community Cloud shall not be available on any other management console.			
18. With respect to monitoring tools, if any agent has to be deployed on the VMs or otherwise, the monitoring tools may be shared provided there is logical segregation and controls built-in to ensure that the tools & deployed agents comply to the security policies and ONLY the events, performance threshold alerts and inventory data for the OS, DB, infrastructure and Application is captured & sent by the deployed agents. The monitoring tools and deployed agents (in case of agent-based tools) shall not capture or send Government Department's application and/or user and/or transaction data	Y	Y	Y
19. All the physical, environmental and security features, compliances and controls of the Data Center facilities (as required under this RFP) shall be enabled for the Cloud Service Offerings	Y	Y	Y
20. Shall leverage and share all network related security toolset which are in network flow However, host based security like IDS, PIM, FIM should be specific to Government Virtual Private Cloud.	N	Y	N
21. Security toolset, except DDOS, shall be a dedicated installation of the tools / products for the Government Community Cloud. DDOS need not be a dedicated installation for the	N	N	Y

Government Community Cloud and may be deployed as a shared service.			
22. Cloud provisioning toolset can be shared tools	Y	Y	N
23. In case, the CSP provides Database System Software as a Service for the Government Department, the database shall be a dedicated instance for the Government Community Cloud.	N	Y	N
24. In case, the CSP provides Database System Software as a Service for the Government Department, the database shall be a dedicated installation for the Government Community Cloud.	N	N	Y
25. For ensuring strategic control of the operations, the CSP shall provide self-service tools to the Government Departments that can be used by the Departments to manage their cloud infrastructure environments including Government Department specific configurations	Y	Y	Y
26. For ensuring strategic control of the operations, approval of the DeitY/Government Departments shall be taken prior to making changes / modifications of the deployed solution, database, data, configurations, security solutions, hosted infrastructure, etc of the Government Community Cloud where such changes affect solutions of multiple Government Departments using the Government Community Cloud. The above set of activities where prior approvals of the DeitY have to be taken is only indicative and by no means an exhaustive list. The set of activities	N	N	Y

for which such approval has to be obtained will be finalized by DeitY/Government Department and reviewed on as needed basis.			
27. Where required, DeitY or the Government Department as applicable, shall be provided the access rights on the cloud services console that will enable authorized DeitY user or Government Department user, as applicable, to approve any critical changes to the solution including the underlying infrastructure before they are carried out by the CSP	N	N	Y
28. For any changes (including auto-provisioning and others that may or may not need prior approval) to the underlying cloud infrastructure, software, etc. under the scope of the CSP, that has the potential to affect the SLAs (performance, availability,..), the Government Department shall get alerts / notifications from the CSP, both as advance alerts and post implementation alerts.	Y	Y	Y

5.2. General Requirements

The below mandatory requirements are applicable for all cloud deployment models.

1. Shall be in accordance with the requirements in this RFP (including the applicable terms and conditions in the Service Level Agreement and Master Services Agreement)
2. There should be at least 30% headroom (at an overall level in the compute & Storage capacity offered) available for near real time provisioning during any unanticipated spikes in the user load.
3. Ability to integrate fully with the Government of India approved Certificate Authorities to enable the Government Departments use the Digital Certificates / Digital Signatures.
4. The respective Government Department shall retain ownership of any user created/loaded data and applications hosted on CSP's infrastructure and maintains the right to request (or should be able to retrieve) full copies of these at any time.
5. The respective Government Department retains ownership of all virtual machines, templates, clones, and scripts/applications created for the department's application. The respective Government Department retains the right to request (or should be able to retrieve) full copies of these virtual machines at any time.
6. The respective Government Department retains ownership of Department loaded software installed on virtual machines and any application or product that is deployed on the Cloud by the Government Department.
7. The respective Government Department shall be provided access rights (including the underlying secure connection) to the user administration / portal of cloud services to have visibility into the dashboard, SLAs, management reports, etc. provided by the Cloud Service provider.
8. CSP shall not provision any unmanaged VMs for the applications.
9. CSPs shall provide interoperability support with regards to available APIs, data portability etc. for the Government Department to utilize in case of Change of cloud service provider, migration back to in-house infrastructure, burst to a different cloud service provider for a short duration or availing backup or DR services from a different service provider.
10. Should adhere to the ever evolving guidelines as specified by CERT-In (http://www.cert-in.org.in/)

11. Should adhere to the relevant standards published (or to be published) by DeitY or any standards body setup / recognized by Government of India and notified to the CSP by DeitY as a mandatory standard.
12. CSP shall also adhere to the relevant audit requirements as defined in the RFP.
13. DeitY has initiated the process of identification of the Standards, develop the necessary specifications, frameworks and guidelines with the help of a Cloud Management Office (CMO). The provisionally accredited cloud service offerings will have the option to comply with the full-fledged guidelines & standards as and when the such guidelines / standards are published by DeitY to get the full accreditation within the timeframe given by DeitY. CSP is responsible for all costs associated with implementing, assessing, documenting and maintaining the accreditation.
14. In case of any delay in publishing full-fledged guidelines / standards by CMO or identification of any critical gaps or deemed as required by DeitY during the period of provisional accreditation, additional guidelines / standards may be published by DeitY from time to time that will be applicable for the Provisionally Accredited Cloud Service Offerings. Provisionally accredited cloud service offerings must comply with the additional guidelines / standards (applicable for the Provisionally Accredited Cloud Service Offerings) as and when such guidelines / standards are published by DeitY at no additional cost to retain the provisional accreditation status. Private Service Providers will be given sufficient time and notice period to comply to the additional guidelines / standards. Any downtime during such approved upgrades will be considered as approved downtime for SLA calculations.
15. Government Department has the option to extend the Provisional Accreditation duration on expiry, to avail the services of the CSP for continuation of the services without the need to go for a separate accreditation process. The duration of extension will be decided by Government Department and will be up to a maximum of one year. The decision on the extension will be taken exclusively by Government Department keeping in consideration a) satisfactory performance of the Agency b) time constraints or other serious impediments in initiation / completion of full-fledged accreditation process c) technological reasons d) Where circumstances inescapably require taking recourse to this option.

5.3. Service Management and Provisioning Requirements

The below mandatory requirements are applicable for all cloud deployment models.

Service Management and Provisioning requirements address the technical requirements for supporting the provisioning and service management of the Cloud Service Offerings proposed to be accredited. Service provisioning focuses on capabilities required to assign services to users, allocate resources, and services and the monitoring and management of these resources.

5.3.1. Service Provisioning

1. Provide the ability to provision virtual machines, storage and bandwidth dynamically (or on-demand), on a self-service mode or as requested.
2. Enable Service Provisioning via online portal/interface (tools).
3. Enable Service Provisioning via Application Programming Interface (API).
4. Secure provisioning, de-provisioning and administering [such as Secure Sockets Layer (SSL)/Transport Layer Security (TLS) or Secure Shell (SSH)]
5. Support the terms of service requirement of terminating the service at any time (on-demand).
6. Provide a webpage and associated Uniform Resource Locator (URL) that describes the following:
    a. Service Level Agreements (SLAs)
    b. Help Desk and Technical Support
    c. Resources (Documentation, Articles/Tutorials, etc)
7. Make the Management Reports described in this RFP accessible via online interface. These reports shall be available for one year after being created.
8. The CSP is expected to carry out the capacity planning in advance to identify & provision, where necessary, the 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.
9. The CSP shall ensure that effective Remote Management features exist so that issues can be addressed by the Government Department in a timely and effective manner.

10. Service Provisioning shall be available via the SSL VPN clients only as against the public internet.

5.3.2. Service Level Agreement Management

1. Provide a robust, fault tolerant infrastructure with enterprise grade SLAs with an assured uptime of 99.5%, SLA measured at the VM Level & SLA measured at the Storage Levels
2. Document and adhere to the SLAs to include:
   a. Service Availability (Measured as Total Uptime Hours / Total Hours within the Month) displayed as a percentage of availability up to one-tenth of a percent (e.g. 99.5%)
   b. Within a month of a major outage occurrence resulting in greater than 1-hour of unscheduled downtime. Describe the outage including description of root-cause and fix.
   c. Service provisioning and de-provisioning times (scale up and down) in near real- time
3. Helpdesk and Technical support services to include system maintenance windows
4. CSP shall implement the monitoring System including any additional tools required for measuring and monitoring each of the Service Levels as per the SLA between the Government Department and the CSP.

5.3.3. Operational Management

1. Manage the network, storage, server and virtualization layers, to include performance of internal technology refresh cycles applicable to meet the SLAs
2. Provide a secure, dual factor method of remote access which allows the Government Department designated personnel (privileged users) the ability to perform duties on the hosted infrastructure
3. Upgrade and periodically replace hardware without financial impact to the Government Department. All the data within it shall be immediately deleted/destroyed and certify the VM and data destruction to the Government Department as per stipulations and shall ensure that the data cannot be forensically recovered.
4. Perform patch management appropriate to the scope of their control

a. Alerts on the upcoming patches via email and management portal, and ability to defer or reject patches before they are applied in the next patch cycle
b. Patch approved VMs on the next available patch management change window;
c. Application of automated OS security patches, unless deferred or rejected by DeitY
d. Send regular approval reminders to DeitY and the Government Department designated email address five (5) days prior to patch cut-off dates

5. OS level vulnerability management – all OS images created within the cloud platform are regularly patched with the latest security updates
6. Provide the artifacts, security policies and procedures demonstrating its compliance with the Security Assessment and Authorization requirements as described in Security Requirements in this RFP.
7. Monitor availability of the servers, CSP -supplied operating system & system software, and CSP's network
8. The CSP is fully responsible for tech refreshes, patch management and other operations of infrastructure that is in the scope of the CSP.
9. Investigate outages, perform appropriate corrective action to restore the hardware, operating system, and related tools
10. CSP should manage CSP provisioned infrastructure including VMs as per the ITIL standards.
11. Comply with technology refresh requirements as required by the DeitY to ensure security requirements and service level agreements (SLA) are met
12. Software within the CSP's scope will never be more than two versions behind unless deferred or rejected by DeitY.

5.3.4. Data Management

1. Manage data isolation in a multi-tenant environment.
2. The CSP should provide tools and mechanism to the Government Department or its appointed agency for defining their backup requirements & policy.
3. The CSP should provide tools and mechanism to the Government 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.

4. Transfer data back in-house either on demand or in case of contract or order termination for any reason
5. Manage data remanence throughout the data life cycle.
6. Provide and implement security mechanisms for handling data at rest and in transit.
7. CSP shall not delete any data at the end of the agreement (for a maximum of 45 days beyond the expiry of the Agreement) without the express approval of the Government Department.
8. When the Government Department or CSP (with prior approval of the Government Department) scales down the infrastructure services, CSP is responsible for deleting or otherwise securing Government Department's Content/data prior to VM deletion and in case deleted, shall ensure that the data cannot be forensically recovered.

5.4. User/Admin Portal Requirements

The below mandatory requirements are applicable for all cloud deployment models.

1. Utilization Monitoring
   a. Provide automatic monitoring of resource utilization and other events such as failure of service, degraded service, etc. via service dashboard or other electronic means.
   b. Real time performance thresholds
   c. Real time performance health checks
   d. Real time performance monitoring & Alerts
   e. Historical Performance Monitoring
   f. Capacity Utilization statistics
   g. Cloud Resource Usage including increase / decrease in resources used during auto-scale
2. Trouble Management
   a. Provide Trouble Ticketing via online portal/interface (tools).
   b. Provide Trouble Ticketing via API.
3. User Profile Management

a. Support maintenance of user profiles and present the user with his/her profile at the time of login

5.5. Integration Requirements

The below mandatory requirements are applicable for all cloud deployment models.

1. Provide support to all Application Programming Interfaces (APIs) including REST API that CSP develops/provides.

5.6. LAN / WAN Requirements

The below mandatory requirements are applicable for all cloud deployment models.

1. Local Area Network (LAN) shall not impede data transmission..
2. Provide a redundant local area network (LAN) infrastructure and static IP addresses from customer IP pool or "private" non-internet routable addresses from CSP pool.
3. Ability to deploy VMs in multiple security zones, as required for the project, defined by network isolation layers in the Customer's local network topology
4. Provide access to Wide Area Network (WAN)
5. Provide private connectivity between a Government Department's network and Data Center Facilities
6. IP Addressing:
   a. Provide IP address assignment, including Dynamic Host Configuration Protocol (DHCP).
   b. Provide IP address and IP port assignment on external network interfaces.
   c. Provide dedicated virtual private network (VPN) connectivity.
   d. Allow mapping IP addresses to domains owned by the Government Department, allowing websites or other applications operating in the cloud to be viewed externally as Government URLs and services.
7. Provide infrastructure that is IPv6 compliant.

8. CSP shall support for providing the secure connection to the Data Center and Disaster Recovery Center (where applicable) from the Government Department Offices.
9. The data center and disaster recovery centre facilities (where applicable) should support connection to the wide area network through high bandwidth links of appropriate capacity to take care of the needs of various types of user entities. Provision has to be made for segregation of access path among various user categories.
10. Support dedicated link to the offices of the Government Department to access the data center and a separate internet link for the other external stakeholders to get access to Government Department services.
11. CSP shall have the capability to provide adequate bandwidth between Primary Data Center and Disaster Recovery Center for data replication purpose.
12. Support network level redundancy through MPLS lines from two different service providers, alternate routing paths facilitated at ISP backbone (MPLS), redundant network devices etc. These two network service providers should not share same back end infrastructure. Redundancy in security and load balancers, in high availability mode, will be provided to facilitate alternate paths in the network

5.7. Data Center Facilities Requirements

The below mandatory requirements are applicable for all cloud deployment models.

1. The data center facilities shall cater for the space, power, physical infrastructure (hardware).
2. The data center facilities and the physical and virtual hardware should be located within India
3. The space allocated for hosting the infrastructure in the Data Center should be secure and exclusively earmarked.
4. The Data Center should be certified for the latest version of ISO 27001 (year 2013) and provide service assurance and effectiveness of Management compliant with SSAE 16 / ISAE 3402 standards
5. The NOC offered for the Data Center Facilities must be within India and the managed services quality should be certified for ISO 20000:1

6. The Data Center should conform to at least Tier III standard (preferably certified under TIA 942 or Uptime Institute certifications by a 3rd party) and implement tool-based processes based on ITIL standards
7. All the physical, environmental and security features, compliances and controls of the Data Center facilities (as required under this RFP) shall be enabled for the environment used for offering cloud services.
8. Provide staff, technical and supervisory, in sufficient numbers to operate and manage the functioning of the DC & DRC with desired service levels
9. Physical Security Standards as per the latest version of ISO 27001 (year 2013) standards.
10. Facility shall be certified (either with respect to Tier Standards or Physical Security Standards) by a Third Party at regular intervals indicating the conformance to the Tier III standards.

5.8. Cloud Storage Service Requirements

The below mandatory requirements are applicable for all cloud deployment models.

The service shall be available online, on-demand, and dynamically scalable up or down per request for service from the end users (Government Department or Government Department's nominated agencies) via SSL VPN clients only as against the public internet through a web browser.

1. Service shall provide scalable, redundant, dynamic storage
2. Service shall provide users with the ability to procure and use storage capabilities remotely via the SSL VPN clients only as against the public internet.
3. Service shall provide storage capabilities on-demand, dynamically scalable per request and via the SSL VPN clients only as against the public internet
4. Storage Space: Online, on-demand virtual storage supporting a single storage sizes of up to 5GB
5. Data Transfer Bandwidth: Bandwidth utilized to transfer files/objects in/out of the providers infrastructure supporting a minimum of 100GB of data transferred (in and out) via the network.
6. There shall not be any additional costs associated with data transfer over and above the ordinary bandwidth charges, or for bulk transfer for Government Department.

5.9. Virtual Machine Requirements

The below mandatory requirements are applicable for all cloud deployment models.

The service shall be available online, on-demand and dynamically scalable up or down per request for service from the end users (Government Department or Government Department's nominated agencies) via SSL VPN clients only as against the public internet through a web browser.

1. Service shall provide auto-scalable, redundant, dynamic computing capabilities or virtual machines.
2. Service shall allow Government Department authorized users to procure and provision computing services or virtual machine instances online via the SSL VPN clients only as against the public internet.
3. Service shall allow users to securely and remotely load applications and data onto the computing or virtual machine instance from the SSL VPN clients only as against the public internet.
4. Perform an Image backup of Customer VM Image information or support the ability to take an existing running instance or a copy of an instance and export the instance into a DeitY approved image format.
5. Configuration and Management of the Virtual Machine shall be enabled via a Web browser over the SSL VPN clients only as against the public internet
6. In case of suspension of a running VM, the VM shall still be available for reactivation for a reasonable time without having to reinstall or reconfigure the VM for the Government Department solution. In case of suspension beyond a reasonable time, all the data within it shall be immediately deleted / destroyed and certify the VM and data destruction to the Government Department as per stipulations and shall ensure that the data cannot be forensically recovered.
7. CSP shall ensure that VMs receive OS patching, health checking, Systematic Attack Detection and backup functions.
8. Monitor VM up/down status and resource utilization such as RAM, CPU, Disk, IOPS and network
9. CPU (Central Processing Unit) - CPU options shall be provided as follows:
    a. A minimum equivalent CPU processor speed of 2.4GHz shall be provided.
    b. The CPU shall support 64-bit operations

10. Provide hardware or software based virtual load balancer Services (VLBS) through a secure, hardened, redundant CSP Managed Virtual Load Balancer platform
11. Provide hardware based load balancing as a service to provide stateful failover and enable Customers to distribute traffic load across multiple servers.
12. Support Clustering
13. Operating System (OS)
    a. Service shall support one or more of the major OS such as Windows, LINUX.
    b. Management of the OS processes and log files including security logs retained in guest VMs;
    c. Provide anti-virus protection;
    d. Provide OS level security as per CSP standard operational procedures as defined in the Information Security Controls for Cloud Managed Services and supporting documentation;
14. Persistence
    a. Persistent Bundled Storage is retained when the virtual machine instance is stopped or
    b. Non-Persistence – Non-Persistence Bundled Storage is released when the virtual instance is stopped. If quoting Non-Persistence VM, the CSP shall provide VM Block storage
15. RAM (Random Access Memory): Physical memory (RAM) reserved for virtual machine instance or Computing supporting a minimum of 1GB of RAM. Memory (RAM) requirement should be different for different type of servers such as web servers and database servers.
16. Disk Space options allocated for all virtual machines and file data supporting a minimum of 40GB bundled storage.
17. Virtual Machine Block Storage Service Requirements
    a. Service shall provide scalable, redundant, dynamic Web-based storage
    b. Service shall provide users with the ability to procure and provision block storage capabilities for cloud virtual machines remotely via the SSL VPN clients only as against the public internet.
    c. Service shall provide block storage capabilities on-demand, dynamically scalable per request for virtual machine instances.
    d. Block Storage – Once mounted, the block storage should appear to the virtual machine like any other disk

e. Storage Space: Online, on-demand storage volumes of arbitrary size ranging from 1 GB to at least 1 TB

f. Input/Output (I/O) Requests: Input/Output requests on block storage

18. Government Department retains ownership of all virtual machines, templates, clones, and scripts/applications created for the Department's application
19. Government Department retains the right to request full copies of these virtual machines at any time.
20. Government Department retains ownership of Department loaded software installed on virtual machines and any application or product that is deployed on the Cloud by the Government Department.
21. Support a secure administration interface - such as SSL/TLS or SSH - for the Government Department designated personnel to remotely administer their virtual instance
22. Provide the capability to dynamically allocate virtual machines based on load, with no service interruption
23. Provide the capability to copy or clone virtual machines for archiving, troubleshooting, and testing
24. Provide capability to perform live migrations (ability to move running VM's) from one host to another.
25. Cloud provider should offer fine-grained access controls including role based access control, use of SSL certificates, or authentication with a multi-factor authentication.
26. 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.
27. Government Department should be permitted to bring and upload additional properly licensed non-operating system software for operation in cloud as required for the Government Department solution for use within the Services by installing it directly on a VM.
28. RAM or CPU of virtual machine should scale automatically whenever there is spike in load to deliver application availability even during spike in load.
29. Provide facility to configure virtual machine of required vCPU, RAM and Disk.
30. Provide facility to use different types of disk like SAS, SSD based on type of application.

5.10. Disaster Recovery & Business Continuity Requirements

1. CSP is responsible for Disaster Recovery Services so as to ensure continuity of operations in the event of failure of primary data center of the Government Department and meet the RPO and RTO requirements. RPO should be less than or equal to 2 hours and RTO shall be less than or equal to 4 hours. The key transaction data shall have RPO of 15 minutes. However, during the change from Primary 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 CSP will be responsible for sizing and providing the DC-DR replication link so as to meet the RTO and the RPO requirements.
2. The Primary DC (of the Government Department) and the DRC should be in different seismic zones
3. During normal operations, the Primary Data Center (of the Government Department) will serve the requests. The Disaster Recovery Site will not be performing any work but will remain on standby. During this period, the compute environment for the application in DR shall be available but with minimum possible compute resources required for a functional DR as per the solution offered. The application environment shall be installed and ready for use. DR Database Storage shall be replicated on an ongoing basis and shall be available in full (100% of the PDC) as per designed RTO/RPO and replication strategy. The storage should be 100% of the capacity of the Primary Data Center site.
4. In the event of a site failover or switchover, DR site will take over the active role, and all requests will be routed through that site. 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. 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 Compute DR environment can be for specific periods during a year for the purposes of 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 Data center. Users of application should be routed seamlessly from DC site to DR site. The CSP shall conduct 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.

5. The CSP shall clearly define the procedure for announcing DR based on the proposed DR solution. The CSP shall also clearly specify the situations in which disaster shall be announced along with the implications of disaster and the time frame required for migrating to DR. The CSP shall plan all the activities to be carried out during the Disaster Drill and issue a notice to the Department at least two weeks before such drill.
6. The CSP should offer dashboard to monitor RPO and RTO of each application and database.
7. The CSP should offer switchover and switchback of individual applications instead of entire system.
8. Any lag in data replication should be clearly visible in dashboard and alerts of same should be sent to respective authorities.

5.11. Security Requirements

The below mandatory requirements are applicable for all cloud deployment models.

1. CSP is responsible for provisioning, securing, monitoring, and maintaining the hardware, network(s), and software that support the infrastructure and present Virtual Machines (VMs) and IT resources to the Government Department. On its part, the Government Department is responsible for the security of the "guest" Operating System (OS) and any additional software, up to and including the applications running on the guest OS.
2. In case, the CSP provides some of the System Software as a Service for the project, CSP is responsible for securing, monitoring, and maintaining the System and any supporting software. Government Department is responsible for securing and maintaining the Government Department application.
3. The Data Center Facility shall at a minimum implement the security toolset: Security & Data Privacy (Data & Network Security including Anti-Virus, Virtual Firewall, Single Sign-on, UTM, One Time Passwords, Multi Factor Authentication, Log Analyzer / Syslog, SSL, DDOS Protection, HIDS / NIDS, Rights Management, SIEM, Integrated Vulnerability Assessment, SOC, Private Virtual Zones, Web Application Filter for OWASP Top 10

protection, Data Privacy, Data Encryption, Certifications & Compliance, Authentication & Authorization, and Auditing & Accounting)

4. Meet the ever evolving security requirements as specified by CERT-In (http://www.cert-in.org.in/)
5. Meet any security requirements published (or to be published) by DeitY or any standards body setup / recognized by Government of India from time to time and notified to the CSP by DeitY as a mandatory standard
6. DeitY and Government Department reserves the right to verify the security test results.
    a. In case of the Government Community Cloud, DeitY and Government Department reserves the right to verify the infrastructure.
7. Implement industry standard storage strategies and controls for securing data in the Storage Area Network so that clients are restricted to their allocated storage.
8. Deploy public facing services in a zone (DMZ) different from the application services. The Database nodes (RDBMS) should be in a separate zone with higher security layer.
9. Ability to create non-production environments and segregate (in a different VLAN) non-production environments from the production environment such that the users of the environments are in separate networks.
10. Cloud offering should have built-in user-level controls and administrator logs for transparency and audit control
11. Cloud Platform should be protected by fully-managed Intrusion detection system using signature, protocol, and anomaly based inspection thus providing network intrusion detection monitoring.
12. Cloud platform should provide Edge-to-Edge security, visibility and carrier-class threat management and remediation against security hazards like Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, botnets, etc. Also, shall provide protection against network issues such as traffic and routing instability.
13. Cloud platform should provide Web Application Filter for OWASP Top 10 protection
14. Access to Government Department provisioned servers on the cloud should be through SSL VPN clients only as against the public internet.
15. Provision of private network ports to be connected to Government Department network for additional secure connectivity between Government Department network and the cloud through support for MPLS, Fiber, P2P links.
16. Virtual Machines should not have console access.

17. Cloud Service provider shall allow audits of all administrator activities performed by Government Department and allow Government Department to download copies of these logs in CSV format.
18. Maintain the security features described below, investigate incidents detected, undertake corrective action, and report to Government Department, as appropriate
19. Deploy and update commercial anti-malware tools (for systems using Microsoft operating systems), investigate incidents, and undertake remedial action necessary to restore servers and operating systems to operation.
20. Shall provide consolidated view of the availability, integrity and consistency of the Web/App/DB tiers
21. CSP should enforce password policies (complex password, change password in some days etc)
22. Shall be contractually subject to all GoI IT Security standards, policies, and reporting requirements. The CSP shall meet and comply with all GoI IT Security Policies and all applicable GoI standards and guidelines, other Government-wide laws and regulations for protection and security of Information Technology.
23. Shall generally and substantially and in good faith follow GoI guidelines and CERT-In and DeitY Security guidance. Where there are no procedural guides, use generally accepted industry best practices for IT security.
24. Information systems must be assessed whenever there is a significant change to the system's security posture
25. Conduct regular independent third party assessments of the CSP's security controls to determine the extent to which security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements and submit the results to DeitY and Government Department
26. Provide an independent Security Assessment/Risk Assessment
27. DeitY reserves the right to perform Penetration Test. If the DeitY exercises this right, the CSP shall allow DeitY's designated third party auditors to conduct activities to include control reviews that include but are not limited to operating system vulnerability scanning, web application scanning, and database scanning of applicable systems that support the processing, transportation, storage, or security of Department's information. This includes the general support system infrastructure.
28. Identified gaps shall be tracked for mitigation in a Plan of Action document.

29. CSP is responsible for mitigating all security risks found and continuous monitoring activities. All high-risk vulnerabilities must be mitigated within 30 days and all moderate risk vulnerabilities must be mitigated within 90 days from the date vulnerabilities are formally identified. The Government will determine the risk rating of vulnerabilities.
30. Shall provide access to the DeitY or their designee acting as their agent, when requested, in order to verify compliance with the requirements for an Information Technology security program. DeitY reserves the right to conduct on-site inspections. CSP shall make appropriate personnel available for interviews and documentation during this review. If documentation is considered proprietary or sensitive, these documents may be reviewed on-site under the CSP's supervision.
31. Shall provide vulnerability scan reports from Web Application, Database, and Operating System Scans. Scan results shall be managed and mitigated in Plans of Action.
32. All documents produced for the project are the property of the Government Department and cannot be reproduced, or retained by the CSP. All appropriate project documentation will be given to Government Department during and at the end of this contract or at the time of termination of the contract. The CSP shall not release any information without the written consent of the Government Department. Any request for information relating to the Project presented to the CSP must be submitted to the Government Department for approval.
33. CSP shall protect all Government Department data, equipment, etc., by treating the information as sensitive. Sensitive but unclassified information, data, and/or equipment will only be disclosed to authorized-personnel. The CSP shall keep the information confidential, use appropriate safeguards to maintain its security in accordance with minimum standards. When no longer required, this information, data, and/or equipment shall be returned to Government Department control, destroyed, or held until otherwise directed by the Government Department. The CSP shall destroy unneeded items by burning, shredding, or any other method that precludes the reconstruction of the material.
34. DeitY has the right to perform manual or automated audits, scans, reviews, or other inspections of the CSP's IT environment being used to provide or facilitate services for the Government Department through a third party auditor appointed or authorized by DeitY. CSP shall be responsible for the following privacy and security safeguards:

a. CSP shall not publish or disclose in any manner, without the DeitY's written consent, the details of any safeguards either designed or developed by the CSP under the Agreement or otherwise provided by the GoI & Government Department.

b. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of any non-public Government data collected and stored by the CSP, the CSP shall afford the DeitY logical and physical access to the CSP's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of the request. Automated audits shall include, but are not limited to, the following methods:

   i. Authenticated and unauthenticated operating system/network vulnerability scans

   ii. Authenticated and unauthenticated web application vulnerability scans

   iii. Authenticated and unauthenticated database application vulnerability scans

35. Automated scans can be performed by DeitY or agents acting on behalf of the DeitY, using DeitY specified tools. If the CSP chooses to run its own automated scans or audits, results from these scans may, at the DeitY's discretion, be accepted in lieu of DeitY performed vulnerability scans. In these cases, scanning tools and their configuration shall be approved by the DeitY. In addition, the results of CSP-conducted scans shall be provided, in full, to the DeitY.

36. Submission to regular audits: CSP will submit to regular audits commissioned by DeitY. The purpose of these audits will not only be to ensure conformance with the requirements stated in this RFP, but also to ensure that the implementation is executed in the best of ways to meet the requirements of DeitY. These audits may be conducted by DeitY or any 3rd party auditor appointed by DeitY. CSP will cooperate fully with the auditor. DeitY will inform the CSP of the short-comings if any after the audit is completed; and the CSP will respond appropriately and address the identified gaps.

5.12. Legal Compliance Requirements

The below mandatory requirements are applicable for all cloud deployment models.

1. IT Act 2000 (including 43A) and amendments thereof

2. Meet the ever evolving security requirements as specified by CERT-In (http://www.cert-in.org.in/)
3. Meet any security requirements published (or to be published) by DeitY or any standards body setup / recognized by Government of India from time to time and notified to the CSP by DeitY as a mandatory standard
4. All services acquired under this RFP including data will be guaranteed to reside in India.
5. There shall not be any legal frameworks outside Indian Law applicable to the operation of the service (and therefore the information contained within it).
6. A copy of the contract / MOU (excluding the commercials) between CSP & Government Department for the purpose of the project, aligned to the terms & conditions of the RFP, should be provided to DeitY.
7. DeitY has initiated the process of identification of the Standards, develop the necessary specifications, frameworks and guidelines including the guidelines for full-fledged accreditation of cloud service offerings with the help of a Cloud Management Office (CMO). The guidelines may also include continuous monitoring of the shared systems that can be leveraged by Government to both reduce their security compliance burden and provide them highly effective security services.
    a. The provisionally accredited cloud service offerings will have the option to comply with the full-fledged guidelines & standards as and when the such guidelines / standards are published by DeitY to get the full accreditation within the timeframe given by DeitY.
    b. CSPs should be prepared to submit the necessary artifacts and the independent verification within the timeframe determined by DeitY once the guidelines & standards are published by DeitY.
    c. CSP is responsible for all costs associated with implementing, meeting, assessing, documenting and maintaining the accreditation.
    d. The cost of meeting all requirements, getting accredited and maintaining accreditation is the responsibility of CSP.
    e. If the CSP fails to meet the guidelines & standards as set by GoI within the timeframe set by DeitY, the Government Department reserves the right to terminate the contract and request to move to a different CSP that meets the mandatory guidelines & standards at no additional cost to Government Department. The Exit Management provisions shall come into effect in such a scenario.
8. CSP shall be responsible for the following privacy and security safeguards:

a. CSP shall not publish or disclose in any manner, without the Government Department's written consent, the details of any safeguards either designed or developed by the CSP under the agreement or otherwise provided by the Government Department or Government of India.
b. CSP shall adhere to the privacy safeguards as laid down by the DeitY and Government Department.
c. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of any non-public Government data collected and stored by the CSP, the CSP shall afford the DeitY or its nominated agency access to the CSP's facilities, installations, technical capabilities, operations, documentation, records, and databases.
d. If new or unanticipated threats or hazards are discovered by either the DeitY or Government Department, Government or the CSP, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of CERT-In and the other party.

5.13. Management Reporting Requirements

The below mandatory requirements are applicable for all cloud deployment models.

Deliverables listed below should be accessible via online interface not later than 10 days after the end of the calendar month and available for up to one year after creation. The information shall be available in format approved by DeitY. The CSP shall monitor and maintain the stated service levels as agreed in the Service Level Agreement between the Government Department and the CSP.

1. Service Level Management
    a. Service Level Management Reports (as per the service levels agreed in the Service Level Agreement between the Government Department and the CSP)
    b. Service Availability at the VM & Service Availability at the Storage Level (Measured as Total Uptime Hours / Total Hours within the Month) displayed as a percentage of availability up to one-tenth of a percent (e.g. 99.5%)

c. Text description of major outages (including description of root-cause and fix) resulting in greater than 1-hour of unscheduled downtime within a month

2. Network and Security Administration (including security breaches with classification, action taken by the CSP and current status) related reports
3. Help Desk / Trouble Tickets raised by the DeitY and / or Government Department
   a. Number of Help Desk/customer service requests received.
   b. Number of Trouble Tickets Opened
   c. Number of trouble tickets closed
   d. Average mean time to respond to Trouble Tickets (time between trouble ticket opened and the first contact with customer)
   e. Average mean time to resolve trouble ticket
4. Monthly utilization (including peak and non-peak volumetric details) of the Service Offerings for the respective Government Department
5. Centralized Monitoring & Management and Reporting with:
   a. Alerts on event threshold and policy based actions upon deviations.
   b. Internet & Intranet Data Transfer
   c. Virtual Instances (vCPU, vMemory, Storage and Network Port) configuration and utilization
   d. Storage Volume (Read/Write and IOPS)
   e. Load balancer
   f. Application Services
   g. Database Monitoring
   h. Reports on non-conformance and escalation for privileged access by unauthorized roles/ identities
6. Government Department will have ten (10) business days, to review, accept or reject all deliverables. Any comments made by the Government Department shall be addressed and a revised deliverable submitted within five (5) business days after the receipt of the comments/rejection, unless a further time extension for incorporating the comments is approved by Government Department.
7. Third Party Audit Certification (at the cost of CSP) every six months indicating the conformance to the requirements detailed in this RFP of the accredited cloud service offerings which are being used by the Government Department. In case the accredited cloud service offerings are not deployed for any Government Department, a self-certification every six months indicating the conformance to the requirements detailed

in this RFP, SLA & MSA of the environments & cloud service offerings accredited should be provided to DeitY

8. Any other reports as deemed required by DeitY from time-to-time.

5.14. Exit Management and Transition Requirements

The below mandatory requirements are applicable for all cloud deployment models.

1. 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 the Government Department. It is the prime responsibility of CSP to ensure continuity of service at all times of the Agreement including exit management period and in no way any facility/service shall be affected/degraded .Further, CSP is also responsible for all activities required to train and transfer the knowledge to the Replacement Agency (or Government Department) to ensure similar continuity and performance of the Services post expiry of the Agreement.
2. At the end of the contract period or upon termination of contract, CSP is required to provide necessary handholding and transition support to ensure the continuity and performance of the Services to the complete satisfaction of Government Department.
3. CSP shall support the Government Department in migration of the VMs, data, content and any other assets to the new environment created by the Government Department or any Agency (on behalf of the Government) on alternate cloud service provider's offerings to enable successful deployment and running of the Government Department's solution on the new infrastructure. CSP shall certify the VM, Content and data destruction to the Government Department as per stipulations and shall ensure that the data cannot be forensically recovered. CSP shall have the responsibility to support and assist the Government Department till the Department is able to successfully deploy and access the services from the new environment.
4. CSP shall not delete any data at the end of the agreement (for a maximum of 45 days beyond the expiry of the Agreement) without the express approval of the Government Department.

5. During the exit/transition management process, it is the responsibility of the CSP to address and rectify the problems with respect to migration of the Department application and related IT infrastructure including installation/reinstallation of the system software etc.
6. The ownership of the data generated upon usage of the system, at any point of time during the contract or expiry or termination of the contract, shall rest absolutely with Government Department.
7. During the contract period, the CSP shall ensure that all the documentation required by the Government Department for smooth transition including configuration documents are kept up to date and all such documentation is handed over to the department during the exit management process.

5.15. Managed Services Requirements

Applicable only when one or a combination of IaaS, PaaS, DevOps and VDaaS cloud service offerings of the private service provider (CSP) are proposed to be accredited.

The below are managed services requirements that the CSP may provide to the Government Departments.

5.15.1. Backup Services

1. The CSP should configure, schedule and manage backups of all the data including but not limited to files, folders, images, system state, databases and enterprise applications as per the policy defined by DeitY or the Government Department.
2. The CSP shall be responsible for file system and database backup and restore services. As part of the responsibilities the CSP should:
   a. Perform and store data and file backups (process of duplicating the customers "to-be-backed-up" "Target Data") consisting of an initial full back up with daily incremental backups for files;
   b. For the files, perform weekly backups;
   c. For the databases, perform a twice weekly full database backup, with a three times daily backup of database log files;
   d. Encrypt all backup files and data and manage encryption keys

e. Monitor and manage backup activity;
f. The encrypted backup copy should be moved to off-site at least once daily
g. Restore the requested data with the objective to initiate a minimum of 95 percent of the total number of restore requests per calendar month within a two hour timeframe for data that can be restored from a local copy;
h. Retain inactive versions of backed up flat files for 30 days and the last version of a deleted file for 60 days;
i. Retain database backups for thirty (30) days;
j. Perform administration, tuning, optimization, planning, maintenance, and operations management for backup and restore;
k. Provide and install additional infrastructure capacity for backup and restore, as required; and,
l. Perform backup on the next scheduled backup window in case of any scheduling conflicts between backup and patch management.

5.15.2. Disaster Recovery & Business Continuity Services

1. In addition to the Primary DC, the CSP is responsible for Disaster Recovery Services so as to ensure continuity of operations in the event of failure of primary data center and meet the RPO and RTO requirements. RPO should be less than or equal to 2 hours and RTO shall be less than or equal to 4 hours. The key transaction data shall have RPO of 15 minutes. 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 CSP will be responsible for sizing and providing the DC-DR replication link so as to meet the RTO and the RPO requirements.
2. The Primary DC and the DRC should be in different seismic zones
3. 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 as defined under Section 5.1
   b. General Requirements as defined under Section 5.2
   c. Service Level Agreement Management as defined under Section 5.3.2
   d. Operational Management as defined under Section 5.3.3

e. Data Management as defined under Section 5.3.4
f. User/Admin Portal Requirements under Section 5.4
g. Integration Requirements under Section 5.5
h. LAN / WAN Requirements under Section 5.6
i. Data Center Facilities Requirements under Section 5.7
j. Security Requirements under Section 5.11
k. Legal Compliance Requirements under Section 5.12
l. Management Reporting Requirements under Section 5.13
m. Exit Management and Transition Requirements under Section 5.14

4. In case of any disaster, the security posture of the DR site shall be identical to the posture provided in the DC.
5. The disaster recovery site shall have the similar environment (physical & IT), processes, and controls (security, etc.) as that of the primary DC. During normal operations, the Primary Data Center will serve the requests. The Disaster Recovery Site will not be performing any work but will remain on standby. During this period, the compute environment for the application in DR shall be available but with minimum possible compute resources required for a functional DR as per the solution offered. The application environment shall be installed and ready for use. DR Database Storage shall be replicated on an ongoing basis and shall be available in full (100% of the PDC) as per designed RTO/RPO and replication strategy. The storage should be 100% of the capacity of the Primary Data Center site.
6. In the event of a site failover or switchover, DR site will take over the active role, and all requests will be routed through that site. 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. 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 Compute DR environment can be for specific periods during a year for the purposes of 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 Data center. Users of application should be routed seamlessly from DC site to DR site. The CSP shall conduct 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.

7. The CSP shall clearly define the procedure for announcing DR based on the proposed DR solution. The CSP shall also clearly specify the situations in which disaster shall be announced along with the implications of disaster and the time frame required for migrating to DR. The CSP shall plan all the activities to be carried out during the Disaster Drill and issue a notice to the Department at least two weeks before such drill.
8. The CSP should offer dashboard to monitor RPO and RTO of each application and database.
9. The CSP should offer switchover and switchback of individual applications instead of entire system.
10. Any lag in data replication should be clearly visible in dashboard and alerts of same should be sent to respective authorities.

6. Governance Structure and Roles of the Different Agencies

DeitY is the authorized department in Government of India with regards to accreditation of the cloud service offerings of the private service provider. To monitor the compliance on an on-going basis and address any non-compliances or deviations from the requirements, DeitY will form a suitable Governance mechanism.

Roles and Responsibilities of DeitY or an Agency nominated by DeitY

1. Primary owner of the Provisional Accreditation Process
2. Provisional Accreditation of Services offered by the Cloud Service Providers
3. Setup of GI Cloud Services Directory
4. Publish Provisionally Accredited Cloud Service Offerings on the GI Cloud Services Directory
5. Monitoring and ensuring compliance to the accreditation guidelines by the Cloud Service Providers
6. Review and Approve the new Data Center Facility (or Facilities) submitted by the private service provider that are found compliant to the requirements of the RFP, MSA and any amendments thereof. The above is applicable once the cloud service offerings of the private service provider from the technically qualified (proposed at the time of the bidding) Data Center Facility (or facilities) are accredited by DeitY and the private service provider chooses to offer the accredited cloud service offerings from a different or additional Data Center Facility (or Facilities).
7. Setup the Governance Structure to review and approve changes / modifications of the deployed solution, database, data, configurations, security solutions, hosted infrastructure, etc of the dedicated infrastructure and solutions of the Government Community Cloud where such changes affect solutions of multiple Government Departments using the Government Community Cloud

There will be no payment to the Provisionally Accredited Cloud Service Providers from DeitY.

Roles and Responsibilities of Government Department

1. Evaluate the suitability of applications / services / projects to leverage Cloud Services
2. Capacity Sizing to estimate compute, storage, and network requirements

3. Assessment of the risk and security profile of their application / data / services and identify the appropriate cloud deployment model and cloud service offering.
4. Select a Cloud Service (IaaS, PaaS, DRaaS,…) from the accredited cloud service offerings based on the requirements of the Government Department
5. Enter into a Master Services Agreement and Service Level Agreement with the selected Cloud Service Provider, aligned with the model Master Services Agreement and model Service Level Agreement provided by DeitY.
6. Migrate to cloud services with the assistance from the Cloud Service Provider (or a Managed Services Provider)
7. Management of the Government Department's Solution and relevant configurations on the cloud infrastructure provided by the cloud service provider
8. Monitoring Service Level Agreement (SLAs) and other management reports provided by the Cloud Service Provider
9. Payment to the Cloud Service Provider based on the Service Level Agreement (SLA) and Master Services Agreement (MSA)
10. Review and approve changes / modifications to configurations specific to a Government Department

Roles and Responsibilities of Cloud Service Provider

1. Comply on an on-going basis to the requirements specified under this RFP
2. Comply on an on-going basis to the requirements specified under the RFP, SLA and MSA with the Government Department
3. Submit the details of the proposed Data Center Facility (or Facilities) including the compliance matrix against the relevant requirements for approval to DeitY. The above is applicable once the cloud service offerings of the private service provider from the technically qualified (proposed at the time of the bidding) Data Center Facility (or facilities) are accredited by DeitY and the private service provider chooses to offer the accredited cloud service offerings from a different or additional Data Center Facility (or Facilities).

.

7. Instructions to Bidders

1. **Availability of the RFP Documents**: The RFP can be downloaded from the website given under Section 3. The bidders are expected to examine all instructions, forms, terms, project requirements and other information in the RFP documents. Failure to furnish all information required as mentioned in the RFP documents or submission of a proposal not substantially responsive to the RFP documents in every respect will be at the bidder's risk and may result in rejection of the proposal and forfeiture of the bid security.

2. **Acknowledgement:** The bidders are requested to acknowledge the receipt of the complete set of RFP documents. The bidder shall also indicate the details of the primary and secondary contact persons for all the future interactions during the bidding process. A signed copy of the acknowledgement should be sent to the bid issuer's address provided in the Section 3. A scanned copy of the signed acknowledgement should be emailed to the bid issuer's address provided in the Section 3.

3. **Earnest Money Deposit (EMD):**

    a. Bidders shall submit, along with their Bids, an amount of INR 10 Lakhs (Rupees Ten Lakhs only), as Earnest Money Deposit ("EMD").

    b. EMD can be either in the form of a DD drawn in favour of "Pay and Account officer, Department of Electronics and Information Technology (DeitY)" payable at Delhi OR a Bank Guarantee issued by any of the commercial banks in the format provided in the Annexure 9.

    c. Bid security in any other form will not be accepted.

    d. EMD shall be valid for a period of 225 days from the last date of submission of the bid.

    e. The bid security of all unsuccessful bidders would be refunded by DeitY within three months of the bidder being notified by DeitY as being unsuccessful. The bid security of the successful bidder would be returned upon submission of Performance Guarantee.

    f. No interest shall be payable by DeitY to the Bidder(s) on the bid security amount for the period of its currency.

    g. The bid without adequate bid security / EMD, as mentioned above, will be liable for rejection without providing any further opportunity to the bidder concerned.

h. The bidder shall extend the validity of the EMD on request by DeitY

i. The bid security may be forfeited:

   i. If a bidder withdraws its bid during the period of bid validity or any extension thereof agreed to by the bidder

   ii. In case of a successful bidder, if the bidder fails to acknowledge and accept the Letter of Award of Provisional Accreditation from DeitY in accordance with terms and conditions

   iii. If any of the bidders modify their bid during the validity period

   iv. If the Bidder tries to influence the evaluation process

4. **Pre-Bid Conference:** DeitY will host a Pre-Bid Conference, tentatively scheduled as per the schedule given in section 4 above. The representatives of the interested organizations may attend the pre-bid conference at their own cost. The purpose of the pre-bid conference is to provide bidders with information regarding the RFP and the proposed requirements in reference to the particular RFP. It will also provide each bidder with an opportunity to seek clarifications regarding any aspect of the RFP and the project. The venue for the Pre bid conference is the bid issuer's address provided in Section 3.

5. **Bidder Inquiries and DeitY's responses:**

   a. All enquiries from the bidders relating to this RFP must be submitted in writing exclusively to the contact person notified by DeitY as above in the format specified in Annexure 1 Request for Clarification Format. A copy of the bidder enquiries should also be emailed to the bid issuer's email address provided in the Section 3. The mode of delivering written questions would be through post or email. In no event will DeitY be responsible for ensuring that bidders' inquiries have been received by them. Telephone calls will not be accepted for clarifying the queries.

   b. After the RFP is issued to the bidder, DeitY shall accept written questions/inquiries from the bidders. DeitY will endeavour to provide a complete, accurate, and timely response to all questions to all the bidders. However, DeitY makes no representation or warranty as to the completeness or accuracy of any response, nor does DeitY undertake to answer all the queries that have been posed by the bidders. All responses given by DeitY will be

published on the website given under Section 3. In case the acknowledgement with the necessary details is submitted by the bidder on receipt of the RFP, DeitY may send the clarifications to such bidders through e-mail. All responses given by DeitY will be available to all the bidders. Any email communications sent by bidders to DeitY must be sent to the email address provided in Section 3.

6. **Supplementary Information / Corrigendum / Amendment to the RFP**

   a. If DeitY deems it appropriate to revise any part of this RFP or to issue additional data to clarify an interpretation of the provisions of this RFP, it may issue supplements to this RFP. Such supplemental information, including but not limited to, any additional conditions, clarifications, minutes of meeting, and official communication over email/post will be communicated to all the bidders by publishing on the website given under Section 3. In case the acknowledgement with the necessary details is submitted by the bidder on receipt of the RFP, DeitY may send the supplemental information / corrigendum / amendment to such bidders through e-mail. Any such supplement shall be deemed to be incorporated by this reference into this RFP.

   b. The letters seeking clarifications sent either to all the bidders or to specific bidder as the case may be during the evaluation of technical proposal and the minutes of the meeting recorded during the technical evaluation shall also be deemed to be incorporated by this reference in this RFP.

   c. At any time prior to the deadline (or as extended by DeitY) for submission of bids, DeitY, for any reason, whether at its own initiative or in response to clarifications requested by prospective bidder, may modify the RFP document by issuing amendment(s). All such amendments will be published on the website given under Section 3. In case the acknowledgement with the necessary details is submitted by the bidder on receipt of the RFP, DeitY may send the amendment(s) to such bidders through e-mail. All such amendment(s) will be binding on all the bidders.

   d. In order to allow bidders a reasonable time to take the amendment(s) into account in preparing their bids, DeitY, at its discretion, may extend the deadline for the submission of bids.

7. **Proposal Preparation Costs:** The bidder is responsible for all costs incurred in connection with participation in this process, including, but not limited to, costs incurred in conduct of informative and other diligence activities, participation in meetings/discussions/presentations, preparation of proposal in providing any additional

information required by DeitY to facilitate the evaluation process and all such activities related to the bid process. This RFP does not commit DeitY to award a contract or to engage in negotiations. Further, no reimbursable cost may be incurred in anticipation of award of the contract for implementation of the project.

8. **DeitY's Right to terminate the Process**

    a. DeitY may terminate the RFP process at any time without assigning any reason. DeitY makes no commitments, explicit or implicit, that this process will result in a business transaction with anyone.

    b. This RFP does not constitute an offer by DeitY. The bidder's participation in this process may result in DeitY selecting one or more bidders to engage in further discussions and negotiations towards issue of Letter of Award of Provisional Accreditation. The commencement of such negotiations does not, however, signify a commitment by DeitY to execute a contract or to continue negotiations.

    c. The DeitY has the right to terminate this discussions and negotiations process without assigning any reason and no costs will be reimbursed to the participating bidders.

    d. DeitY reserves the right to reject any request for provisional accreditation and to annul the provisional accreditation process and reject all such requests at any time prior to provisional accreditation, without thereby incurring any liability to the affected applicant(s) or any obligation to inform the affected applicant(s) of the grounds for such decision.

9. **Acceptance of part / whole bid / modification – Rights thereof:** DeitY reserves the right to modify the technical specifications / quantities / requirements / tenure mentioned in this RFP including addition / deletion of any of the item or part thereof after pre-bid and the right to accept or reject wholly or partly bid offer, or, without assigning any reason whatsoever. No correspondence in this regard shall be entertained. DeitY also reserves the unconditional right to place order on wholly or partly bid quantity to successful bidder.

10. **Authentication of Bids:** The original and all copies of the bid shall be typed or written in indelible ink and signed by the Bidder or a person duly authorized to bind the Bidder to the Contract. A certified true copy of the corporate sanctions/approvals authorizing its authorized representative to sign/act/execute documents forming part of this proposal

including various RFP documents and binding contract shall accompany the bid. All pages of the bid, except for un-amended printed literature, shall be initialed and stamped by the person or persons signing the bid.

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

12. **Venue & Deadline for submission of proposals:**

    a. Proposals, in its complete form in all respects as specified in the RFP, must be submitted to DeitY at the address specified in Section 3.

    b. Last Date & Time of submission: Before the date and time stipulated in schedule given in section 4

    c. DeitY may, in exceptional circumstances and at its discretion, extend the deadline for submission of proposals by issuing an addendum. All such addendums will be published on the website given under Section 3. In case the acknowledgement with the necessary details is submitted by the bidder on receipt of the RFP, DeitY may send the addendum(s) to such bidders through e-mail. In such a case of extension, all rights and obligations of DeitY and the bidders previously subject to the original deadline will thereafter be subject to the deadline as extended.

13. **Late Bids:** Bids received after the due date and the specified time (including the extended period if any) for any reason whatsoever, shall not be entertained and shall be returned unopened.

14. **Conditions under which this RFP is issued**

    a. This RFP is not an offer and is issued with no commitment. DeitY reserves the right to withdraw the RFP and change or vary any part thereof at any stage. DeitY also reserves the right to disqualify any bidder, should it be so necessary at any stage for any reason whatsoever.

    b. Timing and sequence of events resulting from this RFP shall ultimately be determined by DeitY.

c. No oral conversations or agreements with any official, agent, or employee of DeitY shall affect or modify any terms of this RFP and any alleged oral agreement or arrangement made by a bidder with any department, agency, official or employee of DeitY shall be superseded by the definitive agreement that results from this RFP process. Oral communications by DeitY to bidders shall not be considered binding on DeitY, nor shall any written materials provided by any person other than DeitY.

d. Neither the bidder nor any of the bidder's representatives shall have any claims whatsoever against DeitY or any of their respective officials, agents, or employees arising out of, or relating to this RFP or these procedures (other than those arising under a definitive service agreement with the bidder in accordance with the terms thereof).

e. The information contained in this document is only disclosed for the purposes of enabling bidders to submit a proposal to DeitY. No part of this document including the Annexures can be reproduced in any form or by any means, disclosed or distributed to any party not involved in the bid process without the prior consent of DeitY except to the extent required for submitting bid. This document should not therefore be used for any other purpose.

15. **Rights to the Content of the Proposal:** All the bids and accompanying documentation submitted as bids against this RFP will become the property of DeitY and will not be returned after opening of the pre-qualification proposals. If any bidder does not qualify in pre-qualification evaluation, the technical proposal shall not be evaluated. DeitY is not restricted in its rights to use or disclose any or all of the information contained in the proposal and can do so without compensation to the bidders. DeitY 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. DeitY has the right to use the services of external experts to evaluate the proposal by the bidders and share the content of the proposal either partially or completely with the experts for evaluation with adequate protection of the confidentiality information of the bidder.

16. **Modification and Withdrawal of Proposals:** No proposal shall be modified or withdrawn in the intervening period between the deadline for submission of proposals and the expiration of the validity period specified by the bidder on the proposal form. Entire bid security may be forfeited if any of the bidders modify or withdraw their bid during the validity period.

17. **Non-Conforming Proposals:** A proposal may be construed as a non-conforming proposal and ineligible for consideration:

    a. If it does not comply with the requirements of this RFP. Failure to comply with the technical requirements, and failure to acknowledge the receipt of amendments, are common causes for holding proposals non-conforming

    b. If a proposal appears to be "canned" presentations of promotional materials that do not follow the format requested in this RFP or do not appear to address the particular requirements of the proposed solution, and any such bidders may also be disqualified

18. **Disqualification:** The proposal is liable to be disqualified in the following cases:

    a. Proposal submitted without bid security;

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

    c. The bidder qualifies the proposal with its own conditions or assumptions;

    d. Proposal is received in incomplete form;

    e. Proposal is received after due date and time;

    f. Proposal is not accompanied by all the requisite documents;

    g. Proposal is not properly sealed or signed;

    h. Information submitted in technical proposal is found to be misrepresented, incorrect or false, accidentally, unwittingly or otherwise, at any time during the processing of the contract (no matter at what stage) or during the tenure of the contract including the extension period of the contract if any;

    i. Bidder tries to influence the proposal evaluation process by unlawful/corrupt/fraudulent means at any point of time during the bid process;

    j. 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;

    k. Bidder fails to acknowledge and accept the Letter of Award of Provisional Accreditation within 30 working days of the date of notice of award or within such extended period, as may be specified by DeitY;

l. Bidders may specifically note that while evaluating the proposals, if it comes to DeitY's 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 for a further period of three years from participation in any of the tenders floated by DeitY;

m. Bidders or any person acting on its behalf indulges in corrupt and fraudulent practices; and

n. In case bidder fails to meet any of the bidding requirements as indicated in this RFP

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

20. **Offer Validity period:** The proposal should remain valid for a period of 180 days from the date of the submission of offer. A proposal valid for a shorter period may be rejected as non-responsive. 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, DeitY may solicit the bidder's consent for an extension of the validity period. The request and the responses thereto shall be made in writing or by fax or email.

21. **Language of Proposals:** The proposal and all correspondence and documents shall be written in English.

22. **Bid Submission Instructions:** The bid should be submitted in three parts :

a. **Pre-qualification Information** - The format for submission of pre-qualification information is provided in **Annexure-4.**

b. **Technical Bid** – The format for submission of technical bids is provided in **Annexure-5**.

Note: *The technical bid should be valid for 180 days from the date of submission.*

c. The pre-qualification information and the technical proposal together with all supporting documents should be submitted in two separate sealed covers. Each cover should be clearly marked to indicate whether it contains pre-qualification information or technical proposal.

d. The two envelopes mentioned above should be placed in a bigger envelope marked "**Response to RFP for Provisional Accreditation of Cloud Service Offerings**" together with the following :

   i. Covering Letter from the Bidder as per the format provided in **Annexure-2**.

   ii. An EMD as per the details provided under Clause (3) of Section 7.

   iii. A letter of authorization supported by Board Resolution/a power of attorney.

e. All the envelopes shall have the name and address of the bidder to enable the proposal to be returned unopened in case it is declared "late" or the proposal does not qualify.

f. The bidders are requested to sign across the envelopes along the line of sealing to ensure that any tampering with the proposal cover could be detected.

g. The envelope containing the bid should be delivered to DeitY by hand or by post at the address given in Section 3 and date given in Section 4.

h. The pre-qualification information and technical proposal should be submitted in both Hardcopy and soft copy formats in the format given in **Annexure-4 and Annexure-5** respectively. The soft copy should be submitted in a CD.

i. If any bidder does not qualify in pre-qualification evaluation, the technical proposal shall not be evaluated.

j. Bidders are requested to submit a bid that is to the point and refrain from providing unwanted information that is not relevant to this bid.

8. Process of Evaluation

1. Pre-Qualification Criteria

a. The bidder will be assessed on the mandatory prequalification criteria specified under **Annexure 3**, and the bidder shall submit the information for Pre-qualification in the form at **Annexure 4**.

b. DeitY will assess the bidders' capabilities against the pre-qualification criteria. Only those bidders' who meet / exceed the pre-qualification criteria shall proceed for technical evaluation.

2. Technical Evaluation Criteria

a. Bidders that satisfy the pre-qualification criteria will be considered for the Technical Evaluation.

b. The Committee shall evaluate the technical proposal to verify the compliance against the requirements in the RFP. The bidder shall submit the Technical Proposal in the form at **Annexure-5**.

3. Bid Opening Process

a. Total transparency will be observed while opening the proposals/bids.

b. DeitY reserves the rights at all times to postpone or cancel a scheduled bid opening.

c. The bids will be opened, in two sessions, one for Bid Security and Pre-Qualification Proposal and one for Technical of those bidders whose Pre-Qualification Proposals qualify, in the presence of bidders' representatives who choose to attend the Bid opening sessions on the specified date, time and address.

d. The bidders' representatives who are present shall sign a register evidencing their attendance. In the event of the specified date of bid opening being declared a holiday for DeitY, the Bids shall be opened at the same time and location on the next working day. Even if there is no representative of the bidder present, DeitY shall go ahead and open the bid of the bidders.

e. During bid opening, preliminary scrutiny of the bid documents will be made to determine whether they are complete, whether required bid security has been furnished, whether the documents have been properly signed, and whether the bids are generally in order. Bids not conforming to such preliminary requirements will be prima facie rejected.

f. The bid security will be opened by DeitY for bid evaluation, in the presence of bidders' representatives who may choose to attend the session on the specified date, time and address. The Bid Security envelope of the bidders will be opened on the same day and time, on which the Pre-Qualification Proposal is opened, and bids not accompanied with the requisite Bid Security or whose Bid Security is not in order shall be rejected.

4. Bid Evaluation and Selection Process

a. The evaluation of the responses to the RFP will be done by an Evaluation committee of DeitY. DeitY may seek help from external advisers for this purpose.

b. DeitY may seek additional information and clarifications from any or all of the Bidders on the Pre-Qualification and Technical Proposal submitted by the Bidder. Any of the additional information or clarifications submitted by the Bidder on the technical proposal should not have any commercial implications.

c. The evaluation shall be strictly based on the information and supporting documents provided by the Bidders in the application submitted by them. It is the responsibility of the Bidders to provide all supporting documents necessary to fulfil the mandatory eligibility criteria. In case, information required by DeitY is not provided by applicant, DeitY may choose to proceed with evaluation based on information provided and shall not request the applicant for further information. Hence, responsibility for providing information as required in this form lies solely with applicant.

d. The Evaluation Committee shall first evaluate the Pre-Qualification Proposal as per the Pre-Qualification Criteria above. The Pre-Qualification proposal shall be evaluated based on the information provided in the Form at **Annexure-4** and the supporting documents submitted.

e. The technical proposals of only those bidders, who qualify in the evaluation of the pre-qualification proposals, shall be opened.

f. Each responsive proposal will be evaluated for compliance against the mandatory requirements in the RFP. Only the bidders, who meet all the mandatory criteria AND are found to be compliant against the requirements in the RFP will be called for awarding the Provisional Accreditation Contract.

g. The committee shall indicate to all the bidders the results of the evaluation through a written communication.

5. Failure to agree with the Terms and Conditions of the RFP: Failure of the successful bidder to agree with the Terms & Conditions of the RFP shall constitute sufficient

grounds for the annulment of the award, in which event DeitY will call for new proposals. The bidder will also forfeit the EMD.

6. Award of Provisional Accreditation

a. The Letter of Award of Provisional Accreditation will be issued by DeitY to the bidders whose proposal conforms to the RFP.

b. DeitY reserves the right to accept or reject any proposal, and to annul the tendering process and reject all proposals at any time prior to award of Provisional Accreditation, without thereby incurring any liability to the affected bidder or bidders or any obligation to inform the affected bidder or bidders of the reasons / grounds for DeitY's action.

c. Prior to the expiration of the validity period, DeitY will notify the successful bidder in writing or by email, to be confirmed in writing by letter, that its proposal has been accepted. The Letter of Award of Provisional Accreditation, notification of award, will constitute the formation of the contract. The successful bidder will be required to acknowledge and accept the Letter of Award of Provisional Accreditation within 30 days of the date of notice of award.

d. DeitY shall have the right to annul the award in case there is a delay of more than 15 days from the fulfillment of conditions precedent in Acknowledgment and Acceptance of the Letter of Award of Provisional Accreditation, for any reasons attributable to the successful bidders. Upon the Award of Accreditation to the successful bidders, DeitY will promptly notify each unsuccessful bidder and return their Bid Security.

e. The successful bidders should Acknowledge and Accept the Award of Accreditation by DeitY within 30 days of the receipt of the award of the letter in the prescribed format based on the terms and conditions contained in this bid document.

7. Provisional Accreditation: The Cloud Service Providers whose service offerings are provisionally accredited will be intimated by DeitY and have to acknowledge and accept the Letter of Award of Provisional Accreditation accepting the terms and conditions laid down in the RFP. After signing the agreement, no variation or modification in the terms of the agreement shall be made except by written amendment signed by both parties.

8. Period of Accreditation: The provisional accreditation shall be initially for two years from the date of accepting the terms and conditions by the accredited cloud service providers. It can be extended through mutual consent for a further period of one year

based on periodic reviews to assess the performance and compliance during the specified duration of accreditation at the same terms and conditions (or as amended during the duration of provisional accreditation by DeitY).

9. **Allocation of Work**

    a. The private service provider shall not assign the project to any other agency, in whole or in part, to perform its obligation under the agreement.

    b. Mere accreditation by DeitY does not guarantee allocation of work.

    c. The Government Department may select from the accredited cloud service offerings of the private service providers.

    d. Provisional Accreditation with DeitY does not guarantee that any or all Bidders shall be awarded any project / assignment as a result of this accreditation.

10. **New Data Center Facilities:** The below is applicable once the cloud service offerings of the private service provider from the technically qualified (proposed at the time of the bidding) Data Center Facility (or facilities) are accredited by DeitY and the private service provider chooses to offer the accredited cloud service offerings from a different or additional Data Center Facility (or Facilities):

    a. The private service provider is required to submit the details of the proposed Data Center Facility (or Facilities) indicating the compliance against the relevant requirements under the RFP and any amendments thereof for approval to DeitY.

9. General Conditions

1. Bidder represents and warrants that it is in compliance with, and shall continue to comply with, all applicable laws, ordinances, rules, regulations, and lawful orders of public authorities of any jurisdiction in which work shall be performed under this Contract (or the Award of Provisional Accreditation).

2. DeitY reserves the right to terminate the contract by giving a notice of one month if the performance of the private service provider is not found satisfactory. The private service provider shall be given a period of thirty days to cure the breach or fulfill the contractual obligations. Failing which DeitY shall notify the private service provider in writing of the exercise of its right to terminate the contract within 14 days, indicating the contractual obligation(s) for which the private service provider is in default.

3. Conflict of Interest

a. Bidder shall furnish an affirmative statement as to the absence of, actual or potential conflict of interest on the part of the Bidder or any prospective subcontractor due to prior, current, or proposed contracts, engagements, or affiliations with DeitY. Additionally, such disclosure shall address any and all potential elements (time frame for service delivery, resource, financial or other) that would adversely impact the ability of the Bidder to complete the requirements as given in the RFP. Please use form given in **Annexure-6** (Undertaking on Absence of Conflict of Interest) for making declaration to this effect.

4. Termination for Default

a. In the event that DeitY believes that the private service provider is in Material Breach of its obligations under the Contract, DeitY may, without prejudice to any other remedy for breach of contract, terminate the Contract in whole or part upon giving a one month's prior written notice to the private service provider. Any notice served pursuant to this Clause shall give reasonable details of the Material Breach, which could include the following events and the termination will become effective:

i. Private service provider becomes insolvent, bankrupt, resolution is passed for the winding up of the private service provider's organization

ii. Information provided to DeitY is found to be incorrect;

iii. Accreditation conditions are not met as per the requirements of the RFP

iv. Misleading claims about the accreditation status are made;

v. If the private service provider fails to perform any other obligation(s) under the contract.

b. In case of such a breach, DeitY will serve a thirty days written notice for curing this Breach. In case the breach continues, after the expiry of such notice period, the DeitY will have the option to terminate the Contract.

c. In the event the DeitY terminates the contract in whole or in part, the Government Department(s) (that have signed the MSA with the private service provider) may procure, upon such terms and conditions as it deems appropriate, services similar to those undelivered, and the private service provider shall be liable to the Government Department(s) for any excess costs for such similar services where such excess costs shall not exceed 10% of the value of the undelivered services. However, the private service provider shall continue performance of the contract with the Government Department to the extent not terminated. On termination, the exit management and transition provisions as per the Master Services Agreement will come into effect.

5. Confidentiality

a. The private service provider will be exposed, by virtue of the contracted activities, to internal business information of DeitY and other Government Departments. The private service provider would be required to provide an undertaking that they will not use or pass to anybody the data/information derived from the project in any form. The private service provider must safeguard the confidentiality of the DeitY's and Government Department's business information, applications and data. For this, private service provider is required to sign Non-disclosure agreement with DeitY and Government Department (for the respective project).

b. Disclosure of any part of the afore mentioned information to parties not directly involved in providing the services requested, unless required to do so by the Court of Law within India or other Statutory Authorities of Indian Government, could result in premature termination of the contract. The DeitY may apart from blacklisting the private service provider, initiate legal action against the private service provider for breach of trust. The private service provider shall also not make any news release, public announcements or any other reference on RFP or contract without obtaining prior written consent from the DeitY.

c. Private service provider shall use reasonable care to protect confidential information from unauthorised disclosure and use.

d. Except as otherwise permitted by this Agreement, neither of the parties may disclose to third parties the contents of this Agreement or any information/report/advice provided by or on behalf of the other that ought reasonably to be treated as confidential and/or proprietary. Parties may, however, disclose such confidential information to the extent that it: (a) is or becomes public other than through a breach of this Agreement, (b) is subsequently received by the receiving party from a third party who, to the receiving party's knowledge, owes no obligation of confidentiality to the disclosing party with respect to that information, (c) was known to the receiving party at the time of disclosure or is thereafter created independently, (d) is disclosed as necessary to enforce the receiving party's rights under this Agreement, or (e) must be disclosed under applicable law, legal process or professional regulations. These obligations shall be valid for a period of 3 years from the date of termination of this Agreement.

6. **Arbitration**: If, due to unforeseen reasons, problems arise during the progress of the contract leading to disagreement between the DeitY and the private service provider (or the Government Department and the private service provider), both the DeitY (or the Government Department as the case may be) and the private service provider shall first try to resolve the same amicably by mutual consultation. If the parties fail to resolve the dispute by such mutual consultation within twenty-one days, then, depending on the position of the case, either DeitY (or the Government Department as the case may be) or the private service provider can give notice to the other party of its intention to commence arbitration and the applicable arbitration procedure will be as per Indian Arbitration and Conciliation Act, 1996, and the venue of the arbitration will be New Delhi (or a city as determined by the Government Department in its MSA).

7. Indemnification

a. There shall be no infringement of any patent or intellectual & industrial property rights by the private service provider as per the applicable laws of relevant jurisdictions, having requisite competence, in respect of the Deliverables or any part thereof, supplied under the Contract. Private service provider shall indemnify the DeitY (and the Government Department) against all cost/claims/legal claims/liabilities arising from third party claim at any time on account of the infringement or unauthorised use of patent or intellectual & industrial property rights of any such parties.

8. **Governing law and Jurisdiction:** This Accreditation Award and any dispute arising from it, whether contractual or non-contractual, will be governed by laws of India and subject to arbitration clause, be subject to the exclusive jurisdiction of the competent courts of New Delhi, India.

9. Limitation of Liability

a. The liability of private service provider (whether in contract, tort, negligence, strict liability in tort, by statute or otherwise) for any claim in any manner related to the Agreement, including the work, deliverables or Services covered by the Agreement, shall be the payment of direct damages only which shall in no event in the aggregate exceed the total contract value (contract with the Government Department). The liability cap given under this Clause shall not be applicable to the indemnification obligations.

b. In no event shall either party be liable for any consequential, incidental, indirect, special or punitive damage, loss or expenses (including but not limited to business interruption, lost business, lost profits, or lost savings) even if it has been advised of their possible existence.

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

10. Relationship

a. Nothing mentioned herein shall be construed as relationship of master and servant or of principal and agent as between the "DeitY" (or the Government Department) and the "Bidder". No partnership shall be constituted between DeitY (or the Government Department) and the Bidder by virtue of this accreditation nor shall either party have powers to make, vary or release their obligations on behalf of the other party or represent that by virtue of this or any other accreditation a partnership has been constituted, or that it has any such power. The Bidders shall be fully responsible for the services performed by them or on their behalf.

b. Neither party shall use the other parties name or any service or proprietary name, mark or logo of the other party for promotional purpose without first having obtained the other party's prior written approval.

11. Fraud and Corruption

a. DeitY requires that the Bidders engaged through this process must observe the highest standards of ethics during the performance and execution of the awarded project(s). The following terms apply in this context:

b. DeitY will reject the application for accreditation, if the applicant recommended for accreditation, has been determined by DeitY to having been engaged in corrupt, fraudulent, unfair trade practices, coercive or collusive.

c. These terms are defined as follows:

   i. "Corrupt practice" means the offering, giving, receiving or soliciting of anything of value to influence the action of DeitY or any Government Department during the tenure of accreditation.

   ii. "Fraudulent practice" means a misrepresentation of facts, in order to influence a procurement process or the execution of a contract, to DeitY, and includes collusive practice among Bidders (prior to or after Proposal submission) designed to establish proposal prices at artificially high or non-competitive levels and to deprive DeitY of the benefits of free and open competition.

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

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

   v. “Collusive practices” means a scheme or arrangement between two or more Bidders with or without the knowledge of the DeitY, designed to establish prices at artificial, non-competitive levels;

d. DeitY will reject an application for award, if it determines that the bidder recommended for award has, directly or through an agent, engaged in corrupt, fraudulent, unfair trade, coercive or collusive practices in competing for any assigned project during the accreditation.

Request for Clarification Format

Bidder's Request for Clarification on RFP			
Name of the Bidder submitting the request		Name and position of person submitting request	Full formal address of the bidder including phone, fax and email points of contact
S. No	RFP Document Reference(s) (section number/ page)	Content of RFP requiring Clarification	Points on which clarification required
1.			
2.			

RFP Response Cover Letter

Original signed copy on company letterhead

[Date]

To,

Mr. Kshitij Kushagra
Scientist D/Joint Director
Department of Electronics and Information Technology
Electronics Niketan , 6, CGO Complex
New Delhi-110 003
Tel: +91-11- 124301423

Dear Sir,

Ref: Response to Request for Proposal for Provisional Accreditation of Cloud Service Offerings of Private Service Providers (CSP)

Having examined the RFP, the receipt of which is hereby duly acknowledged, we, the undersigned, submit our proposal for Provisional Accreditation of Cloud Service Offerings of Private Service Providers (CSP) for the below Cloud Service Offerings:

Cloud Service Offering	Public Cloud	Virtual Private Cloud	Government Community Cloud
IaaS	<Yes / No>	<Yes / No>	<Yes / No>
PaaS	<Yes / No>	<Yes / No>	<Yes / No>
Disaster Recovery as a Service (DRaaS)	<Yes / No>	<Yes / No>	<Yes / No>
Dev / Test Environment as a Service (DevOps)	<Yes / No>	<Yes / No>	<Yes / No>
Virtual Desktops as a Service	<Yes / No>	<Yes / No>	<Yes / No>
Managed Services: Backup Services (OPTIONAL)*	<Yes / No>	<Yes / No>	<Yes / No>

Managed Services: Disaster Recovery & Business Continuity Services (OPTIONAL)*	<Yes / No>	<Yes / No>	<Yes / No>

** Applicable only when one or a combination of IaaS, PaaS, DevOps and VDaaS cloud service offerings of the private service provider (CSP) are proposed to be accredited.*

We agree to abide by this response for a period of six months from the last date for submission of RFP response.

The following persons will be the authorized representative of our company/ organisation for all future correspondence between the DeitY and our organisation.

Organization	Name: Address: Phone:
Primary Contact	Name: Title: Phone: Email:
Secondary Contact	Name: Title: Phone: Email:
Executive Contact	Name: Title: Phone: Email:

We fully understand that in the event of any change in our contact details, it is our responsibility to inform DeitY about the new details. We fully understand that DeitY shall not be responsible for non-receipt or non-delivery of any communication and/or any missing communication from the DeitY to us, in the event that reasonable prior notice of any change in the authorized person(s) of the company is not provided to DeitY.

We confirm that the information contained in this response or any part thereof, including its exhibits, and other documents and instruments delivered or to be delivered to the DeitY is true, accurate, verifiable and complete. This response includes all information necessary to ensure that the statements therein do not in whole or in part mislead DeitY in its short-listing process.

We fully understand and agree to comply that on verification, if any of the information provided here is found to be misleading, we are liable to be dismissed from the selection process or, in the event of our selection, our contract is liable to be terminated.

We agree for unconditional acceptance of all the terms and conditions set out in this RFP document. We hereby declare that in case our cloud services get provisionally accredited, we shall acknowledge and accept the Letter of Award of Provisional Accreditation as per the requirements of the RFP within 30 working days from the date of notice of award.

We agree that you are not bound to accept any response that you may receive from us. We also agree that you reserve the right in absolute sense to reject all or any of the products/ services specified in the RFP response.

It is hereby confirmed that I/We are entitled to act on behalf of our company /corporation/firm/organization and empowered to sign this document as well as such other documents, which may be required in this connection.

Dated this Day of **2015**

(Signature) (In the capacity of)
(Name)

Duly authorized to sign the Tender Response for and on behalf of:

(Name and Address of Company) Seal/Stamp of bidder

Witness Signature:

Witness Name:

Witness Address:

(Company Seal)

CERTIFICATE AS TO AUTHORISED SIGNATORIES

I,,……, the Company Secretary of ……, certify that …… who signed the above Bid is authorized to do so and bind the company by authority of its board/ governing body.

Date:
Signature:

(Company Seal)

(Name)

List of Enclosures:

1. EMD as per the details provided under Clause (3) of Section 7
2. A certified true copy of the corporate sanctions / approvals authorizing its authorized representative to sign/act/execute documents forming part of this proposal including various RFP documents and binding contract
3. Envelop super-scribed "Pre-qualification Information" as per the format provided in Annexure 4
4. Envelop super-scribed "Technical Bid" as per the format provided in Annexure 5

Pre-Qualification Criteria

The Responses received will be evaluated based on the following criteria as specified below.

i. The Bidder, as a single legal entity, must be incorporated and registered in India under the Indian Companies Act 1956 or a Limited Liability Partnership (LLP) registered under the LLP Act, 2008 or Indian Partnership Act 1932 and should have been in operation in India for minimum of three years

ii. The Bidder, as a single legal entity or its holding company, must have a positive Net Worth in each of the last two financial years 2013-14 and 2014-15).

iii. The Bidder, as a single legal entity or its holding company, must have a minimum annual revenue of INR 20 Crores from the Data Centre related services for each of the last two financial years (2013-14 and 2014-15) either in India or Globally.

iv. The Bidder, as a single legal entity or its holding company, should be currently delivering Infrastructure as a Service offering in India or globally (IaaS as per the National Institute of Standards and Technology (NIST) Definition of Cloud Computing definition providing on-demand Storage and VMs). The IaaS offering shall provide for tools or capabilities that enable users to unilaterally provision / order, manage, and use the Cloud services:

    a) Service Management & Provisioning (Service Provisioning and De-Provisioning near real-time of provisioning request, SLA Management, and Utilization Monitoring)

    b) Provide visibility into service via dashboard

    c) User / Admin Portal (User Profile Management, Trouble Management)

    d) Enterprise grade SLAs with an assured uptime of 99.5% (measured as Total Uptime Hours / Total Hours within the Month), SLA measured at the VM Level and SLA measured at the Storage level

    e) Cloud services should be accessible via internet and MPLS

v. The Data Center Facility (or each of the facilities as the case may be[1]) proposed for provisional accreditation (facility from where the cloud service offerings are proposed to be offered) must meet the following criteria:

    a) The Data Center Facility must be within India, should be currently operational and have a minimum capacity of 50 Racks being operational

    b) The Data Center Facility shall at a minimum have:

        i. Routers, Firewalls, LAN, WAN, Internet Access, and Hosting Centers, Backup, Operations Management, and Data Management

        ii. Security & Data Privacy (Data & Network Security including Anti-Virus, Virtual Firewall, Single Sign-on, UTM, One Time Passwords, Multi Factor Authentication, Log Analyzer / Syslog, SSL, DDOS Protection, HIDS / NIDS, Rights Management, SIEM, Integrated Vulnerability Assessment, SOC, Private Virtual Zones, Web Application Filter for OWASP Top 10 protection, Data Privacy, Data Encryption, Certifications & Compliance, Authentication & Authorization, and Auditing & Accounting)

iii. Conform to at least Tier III standard, preferably certified under TIA 942 or Uptime Institute certifications by a 3rd party

iv. Assured protection with security built at multiple levels

v. Certified for the latest version of ISO 27001 (year 2013)

vi. NOC offered for the Data Center and the managed services quality should be certified for ISO 20000:1

vi. The Bidder, as a single legal entity or its holding company, should not be blacklisted for its Data Center Operations by Central Government Ministry or Department of Government of India. Bidder, as a single legal entity or its holding company, also should not be under any legal action for indulging in corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice with any Central Government Ministry or Department of Government of India. The Bidder shall submit a self-declaration on the company letter head, signed by authorized signatory.

1. ***IN CASE THE BIDDER CHOOSES TO OFFER THE CLOUD SERVICES PROPOSED FOR ACCREDITATION FROM MULTIPLE DATA CENTER FACILITIES, EACH OF THE DATA CENTER FACILITIES SHALL MEET THE CRITERIA***

Form for Submission of Prequalification Information

The pre-qualification information should address all the pre-qualification criteria as specified in the Annexure 3 and should contain details of how the bidder satisfies the pre-qualification criteria.

1. **General Details of the Organization**

   a. This part must include a general background of the respondent organization **(limited to 400 words**) providing the details of the relevant services offered by the Organization

2. **Incorporation Details of the Organization**

   a. Incorporation details of the organization as per the format provided below. Enclose the mandatory supporting documents listed in format.

Details of the Organization	
Name of organization	
Nature of the legal status in India	
Legal status reference details	
Nature of business in India	
Date of Incorporation	
Date of Commencement of Business	
Address of the Headquarters	<<street and mailing addresses, phone, fax and email>>
Address of the Registered Office in India	<<street and mailing addresses, phone, fax and email>>
Address of the Data Center Facility	<<street and mailing addresses, phone, fax and email>>
Other Relevant Information	
Mandatory Supporting Documents: a) Certificate of Incorporation from Registrar Of Companies(ROC)	

3. **Incorporation Details of the Holding Company (Only required if the some of the pre-qualification conditions are being met the Bidder's Holding Company)**

   a. Incorporation details of the holding company as per the format provided below.

Details of the Organization	
Name of organization	
Nature of the legal status in India	
Legal status reference details	
Nature of business	
Date of Incorporation	
Date of Commencement of Business	
Address of the Headquarters	<<street and mailing addresses, phone, fax and email>>
Address of the Registered Office in India, if any	<<street and mailing addresses, phone, fax and email>>
Nature of Relationship with the Bidder's Organization (Holding Company – Subsidiary Company Relationship)	
Address of the Data Center Facility	<<street and mailing addresses, phone, fax and email>>
Other Relevant Information	

4. **Financial Details of the Organization**

   a. Financial details of the organization as per format below. Enclose the mandatory supporting documents listed in format.

Financial Information of *<<Bidder / Holding Company>>*		
	FY 2014-15	FY 2013-14
Net Worth (in INR Crores)		
Revenue from the Data Centre related services (in INR Crores)		
Other Relevant Information		
Mandatory Supporting Documents: a. Auditor Certificate for the last two financial years: 2013-14 and 2014-15 indicating the Net Worth and Revenue from the Data Centre related services		

5. Details of the IaaS Cloud Service Offerings either in India or Globally

Details of the IaaS Cloud Service Offerings of *<<Organization / Holding Company>>*	
IaaS services are offered by	Bidder as a Single Legal Entity OR Holding Company of the Bidder
Countries where the IaaS services are offered	
Start date of offering of the Infrastructure as a Service offerings (IaaS as per the National Institute of Standards and Technology (NIST) Definition of Cloud Computing definition providing on-demand Storage and VMs) from the Data Center Facility	Month & Year
Conformance with respect to: The IaaS offering shall provide for tools or capabilities that enable users to unilaterally provision / order, manage, and use the Cloud services	<<Yes / No>>
Other Relevant Information	

6. Details of the Data Center Facility and Cloud Service Offerings in India

(IN CASE THE BIDDER CHOOSES TO OFFER THE CLOUD SERVICES PROPOSED FOR ACCREDITATION FROM MULTIPLE DATA CENTER FACILITIES, PLEASE PROVIDE THE DETAILS OF EACH OF THE DATA CENTER FACILITIES IN THE FORMAT BELOW)

Details of the Data Center Facility	
Address of the Data Center Facility	<<street and mailing addresses, phone, fax and email>>
Month / Year of Starting the Data Center Operations	Month & Year
Operational Capacity (Number of Racks)	<<Number >>
Availability of Routers, Firewalls, LAN, WAN, Internet Access, and Hosting Centers, Backup, Operations Management, and Data Management	<<Yes / No>>
Security Features available including Physical Security (Security & Data Privacy (Data & Network Security including Anti-Virus, Virtual Firewall, Single Sign-on, UTM, One Time Passwords, Multi Factor Authentication, Log Analyzer / Syslog, SSL, DDOS Protection, HIDS / NIDS, Rights Management, SIEM, Integrated	<<Yes / No>>

Vulnerability Assessment, SOC, Private Virtual Zones, Web Application Filter for OWASP Top 10 protection, Data Privacy, Data Encryption, Certifications & Compliance, Authentication & Authorization, and Auditing & Accounting))	
Tier Level and certifications, if any (Conformance to at least Tier III standard, preferably certified under TIA 942 or Uptime Institute certifications by a 3rd party)	<<Yes / No>> In case certified, details of the Certification
Certified for the latest version of ISO 27001 (year 2013)	<<Yes / No>> Details of the Certification
NOC offered for the Data Center and the managed services quality should be certified for ISO 20000:1	<<Yes / No>> Details of the Certification
Other Relevant Information	
Mandatory Supporting Documents: a) ISO 27001 (year 2013) Certification Details b) ISO 20000:1 Certification Details	

7. Self-declaration on the Blacklisting from the bidder in company letter head, signed by authorized signatory

a. The Bidder, as a single legal entiry or its holding company (if applicable), should not be blacklisted for its Data Center Operations by Central Government Ministry or Department of Government of India. Bidder, as a single legal entiry or its holding company (if applicable), also should not be under any legal action for indulging in corrupt practice, fraudulent practice, coercive practice, undesirable practice or restrictive practice with any Central Government Ministry or Department of Government of India. The Bidder shall submit a self-declaration on the company letter head, signed by authorized signatory.

Form for Submission of Technical Bid

The technical proposal should address all the areas/ sections as specified by the RFP and should contain a detailed description of how the bidder will provide the required services outlined in this RFP. It should articulate in detail, as to how the bidder's Technical Solution meets the requirements specified in the RFP. The technical proposal must not contain any pricing information.

The technical proposal shall contain the following:

1. **Undertaking on Absence of Conflict of Interest** as per the format provided under Annexure 6

2. **Undertaking on Legal Compliance** as per the format provided under Annexure 7

3. **Requirements Compliance Matrix against each of the Cloud Service Offerings proposed to be accredited** as per the format provided under Annexure 8

4. **Details (including the overview and implementation details) of Cloud Deployment Models proposed to be accredited**
    a. Public Cloud
    b. Virtual Private Cloud
    c. Government Community Cloud

5. **Service Catalogue including the various details / attributes of Cloud Service Offerings proposed to be accredited**
    a. Infrastructure as a Service (IaaS)
    b. Platform as a Service (PaaS)
    c. Disaster Recovery as a Service (DRaaS)
    d. Dev / Test Environment as a Service (DevOps)
    e. Virtual Desktops as a Service

Undertaking on Absence of Conflict of Interest

Original signed copy on company letterhead

[Date]

To,

Mr. Kshitij Kushagra
Scientist D/Joint Director
Department of Electronics and Information Technology
Electronics Niketan , 6, CGO Complex
New Delhi-110 003
Tel: +91-11- 124301423

Dear Sir,

Ref: Undertaking on Absence of Conflict of Interest

I/We as Bidder do hereby undertake that there is absence of, actual or potential conflict of interest on the part of our organization or any prospective subcontractor due to prior, current, or proposed contracts, engagements, or affiliations with DeitY. I/We also confirm that there are no potential elements (time frame for service delivery, resource, financial or other) that would adversely impact the ability of our organization to comply with the requirements as given in the RFP.

We undertake and agree to indemnify and hold DeitY harmless against all claims, losses, damages, costs, expenses, proceeding fees of legal advisors (on a reimbursement basis) and fees of other professionals incurred (in the case of legal fees & fees of professionals, reasonably) by DeitY and/or its representatives, if any such conflict arises later.

Yours faithfully,

Authorised Signatory

Designation

Undertaking on Legal Compliance

Original signed copy on company letterhead

[Date]

To,

Mr. Kshitij Kushagra
Scientist D/Joint Director
Department of Electronics and Information Technology
Electronics Niketan , 6, CGO Complex
New Delhi-110 003
Tel: +91-11- 124301423

Dear Sir,

Ref: Undertaking on Legal Compliance

I/We as Bidder do hereby comply to the IT Act 2000 (including 43A) and amendments thereof; meet ever evolving Security Guidelines specified by CERT-In, and meet any security requirements published (or to be published) by DeitY or any standards body setup / recognized by Government of India from time to time and notified to the CSP by DeitY as a mandatory standard.

We confirm that all the services acquired under this RFP including data will be guaranteed to reside in India and there shall not be any legal frameworks outside Indian Law that will be applicable to the operation of the service (and therefore the information contained within it).

Yours faithfully,

Authorised Signatory

Designation

Format for Requirement Compliance Matrix

Sr. No.	Minimum Requirements as Provided in the RFP/Addendum	Comply (Y for Yes / N for No)	Details on how the offerings of the Cloud Service Provider meets the requirement
1.	Section 5.1: Deployment Model Specific Requirements		
2.	Section 5.2: General Requirements		
3.	Section 5.3: Service Management and Provisioning Requirements		
4.	Section 5.4: User/Admin Portal Requirements		
5.	Section 5.5: Integration Requirements		
6.	Section 5.6: LAN / WAN Requirements		
7.	Section 5.7: Data Center Facilities Requirements		
8.	Section 5.8: Cloud Storage Service Requirements		
9.	Section 5.9: Virtual Machines Requirements		
10.	Section 5.10: Disaster Recovery & Business Continuity Requirements		
11.	Section 5.11: Security Requirements		
12.	Section 5.12: Legal Compliance Requirements		
13.	Section 5.13: Management Reporting Requirements		
14.	Section 5.14: Exit Management / Transition Requirements		
15.	Section 5.15: Managed Services Requirements (Optional)		

Note:

i. Compliance: The requirements in the RFP contain the expected responsibilities of the bidder. These requirements are intended to elicit the concurrence of the bidder that it will perform the requirement as written. If the bidder has read, understood, and will comply with a requirement exactly as written, the bidder should enter a “Y” or “Yes” in the column to indicate that the bidder will comply with the requirement as written.

Format for Earnest Money Deposit (EMD)

[Date]
From:
Bank _____

To,

Mr. Kshitij Kushagra
Scientist D/Joint Director
Department of Electronics and Information Technology
Electronics Niketan , 6, CGO Complex
New Delhi-110 003
Tel: +91-11- 24301423

1. In consideration of _____ (hereinafter called the "DeitY") represented by _____, on the first part and M/s _____ of _____ (hereinafter referred to as "Bidder") on the Second part, having agreed to accept the Earnest Money Deposit of Rs. _____ (Rupees _____) in the form of Bank Guarantee for the Request for Proposal for Provisional Accreditation of Offerings of Cloud Service Providers (CSPs), we _____ (Name of the Bank), (hereinafter referred to as the "Bank"), do hereby undertake to pay to the DeitY forthwith on demand without any demur and without seeking any reasons whatsoever, an amount not exceeding _____ (Rupees _____) and the guarantee will remain valid up to a period of 225 days from the due date of the tender. It will, however, be open to the DeitY to return the Guarantee earlier than this period to the bidder, in case the bidder has been notified by the DeitY as being unsuccessful.

2. In the event of the bidder withdrawing the tender before the completion of the stages prior to the finalization of the accreditation process or during the accreditation process, as the case may be, the EMD / Bid Security deposited by the bidder stands forfeited to the Government. We also undertake not to revoke this guarantee during this period except with the previous consent of the Government in writing and we further agree that our liability under the EMD / Bid Security shall not be discharged by any variation in the term of the said tender and we shall be deemed to have agreed to any such variation.

3. No interest shall be payable by the DeitY to the bidder on the guarantee for the period of its currency.

4. Notwithstanding anything contained hereinabove:

a) Our liability under this Bank Guarantee shall not exceed and is restricted to Rs._____(Rupees_____only)

b) This Guarantee shall remain in force up to and including _____ .

c) Unless the demand/claim under this guarantee is served upon us in writing before _____ all the rights of DeitY under this guarantee shall stand automatically forfeited and we shall be relieved and discharged from all liabilities mentioned hereinabove.

Dated this_____day of _____ 2015

For the Bank of _____
(Agent/Manager)