MeghRaj CLOUD INITIATIVE

GOVERNMENT OF INDIA

Guidelines for Government Departments for Adoption/ Procurement of Cloud Services

Ministry of Electronics and Information Technology (MeitY)
Electronics Niketan, 6,
CGO Complex New Delhi-110 003

March 31, 2017

This Page is Intentionally Left Blank

Table of Contents

This Page is Intentionally Left Blank

Glossary of Terms

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

This Page is Intentionally Left Blank

1. Background

MeitY has announced MeghRaj Policy to provide strategic direction for adoption of cloud services by the Government (http://meity.gov.in/content/gi-cloud-initiative-meghraj). The aim of the cloud policy is to realize a comprehensive vision of a government cloud (GI 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 MeitY 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."

1.1 Provisional Empanelment of Cloud Service Offerings

Taking demand into consideration, MeitY has initiated Provisional Empanelment of the cloud service offerings of 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 provisionally empanelled cloud service offerings of the Service Providers, will be published through a GI Cloud Services Directory for use by government departments or agencies at the Centre and States.

The following cloud service offerings offered by the Cloud Service Providers (www://meity.gov.in) for a combination of the Deployment Models (Public Cloud, Virtual Private Cloud and Government Community Cloud) have been provisionally empanelled by Meity.

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 provisional empanelment shall be initially for two years from the date of accepting the terms and conditions by the empanelled cloud service providers. The provisionally empanelled cloud service providers will have the option to comply with the full-fledged guidelines / standards to get the certification for their offerings as and when the new guidelines / standards are published by MeitY.

STQC is in the process of auditing and certification of the empanelled services. MeitY has opened up the process of empanelment and henceforth the potential Cloud Service

Providers can apply for empanelment and certification by MeitY. The audited/certified service offerings of various CSPs are available at www.meity.gov.in

To further facilitate the end user departments for procuring/ adopting cloud computing services, MeitY has prepared broad guidelines indicated in the following sections***. The guidelines are provided as a general guidance and Departments should customize the guidelines and formulate the RFP according to the project specific requirements and procurement strategy.***

2. Key Considerations for Cloud Procurement

Cloud computing is becoming an increasingly attractive model for delivery of infrastructure and other services primarily due to its essential characteristics of on-demand self-services, elasticity etc. However, there are differences between traditional on premise procurement process and procurement process for cloud computing. Therefore Departments need to be aware of the key considerations which need to be addressed when procuring cloud services. The key differences are highlighted in the table below:

S.No	Considerations	Conventional IT Projects	Cloud Service Project
1.	Requirements Estimation (compute, storage, memory, software licenses..,)	The Department needs to estimate the requirements for the total duration of the project (forecasting for 3 or 5 years) and indicates the BoM based on the assessed requirements in the RFP	For Cloud Procurement, the Department may not undertake the estimation for the entire project duration. The Minimum / Indicative Day One requirements can be indicated in the RFP
2.	Flexibility to Procure Variable Quantity of the Same Service	For a conventional Project, if the Department has any additional procurement requirements (servers, storage..,) it has to go through the procurement process	The flexibility to scale up/down and the ability to provision virtual machines, storage and bandwidth dynamically enable procurement of additional requirements hassle free.
3.	Scenario Based Pricing	Since the requirements for the entire duration of project need to be specified in the RFP, the pricing becomes a Fixed Price model	For cloud procurement two plausible pricing options are possible: #1- Indicative requirements #2 Minimum Requirements with indicative Peak Load
4.	Payment Model	As a corollary to the requirements and Pricing model, the Payment terms are fixed timelines based payments	With the option of scaling up or down based on the requirements, procurement of cloud services needs a model of Pay-As-You-Go utility model
5.	Shared Responsibility	The Responsibility of the Project and deliverables lies with Selected bidder.	The responsibility of the Project, (owing to critical Security concerns) is shared between the CSP and the Department.

S.No	Considerations	Conventional IT Projects	Cloud Service Project
6.	Standardized SLA	The conventional IT projects have largely well-defined and accepted SLAs across the project domains.	SLAs critical to cloud services need to be identified and to be incorporated in the agreement.
7.	Contractual Clauses	Traditional IT projects have fairly standardized contracts.	Contractual clauses Specific to Cloud need to be addressed in the RFP (Data Location, Legal Compliance, Exit Management..,)

Therefore, in order to create a fast, flexible procurement process that capitalizes on the full scale and flexibility of the cloud, Departments may consider the following key components while procuring Cloud Services.

a. Cloud Services Requirements

b. Security – Shared Responsibility

c. Migration of Existing Systems to Cloud

d. Operational & Monitoring Requirements

e. Exit Management/Transitioning out services

f. Managed Services

g. Role of Government Departments

h. Pay-As-You-Go utility model

i. Evaluation of CSPs

j. Contractual Terms and Service Level Objectives

a. Cloud Service Requirements

The Government Department/Agency need to estimate the resources based on the application, workload etc. The departments need to estimate the requirements of Virtual Machines, Storage etc. for different environment such as Pre-Production (Development, Testing), Production and Disaster Recovery. The Government Department may indicate the Service Model, the details of existing software licenses and any additional requirements over and above the requirements published by Meity in the RFP for Provisional Empanelment Compliance by the CSPs. Additionally the indicative requirements or the minimum assured requirements need to be mentioned to obtain quotes from the CSPs. There are also a variety of tools and resources available with the CSPs to estimate the resources on cloud based on the current / anticipated server, storage configurations and workloads. The Government Department / Agency may utilize such tools along with the envisaged TO BE

architecture to arrive at the estimates for the indicative day-one operating requirements or minimum assured requirements.

b. Security – Shared Responsibility

The CSP and the departments share control over the Cloud environment and therefore both parties have responsibility for managing it. The CSP's part in this shared responsibility includes providing its services on a highly secure and controlled platform and providing a wide array of security features customers can use. The department's responsibility includes configuring their IT environments in a secure and controlled manner for their purposes.

c. Operations and Maintenance Requirements:

Deployment on cloud requires continuous monitoring and management. Migrating to cloud creates a model of shared responsibility between the Government Department / Agency and the Cloud Service Provider. The Government Department / Agency may choose to procure managed services (O&M – Cloud Services) in addition to the Cloud Services to assist in managing the operations on the cloud. The responsibility of operating the IT environment including management, operation, and verification of shared IT controls is shared between the Government Department / Agency and Cloud Service Provider.

d. Exit Management / Transition-Out Services

The responsibilities of the cloud Service Provider during the exit management period need to be clearly delineated in the RFP. The CSP/MSP shall assist the Department in migrating the VMs, data etc., and should ensure destruction of data.

e. Role of Government Departments in Operations Phase

It is essential that the Department monitors the operational activities to ascertain that the MSP/SI has implemented the cloud features mentioned in the RFP. The Departments need to review and validate the security configurations created by the MSP, review the notifications and patches released by the CSP and validate that the same is being taken into consideration by the MSP during operations, confirm that the audit trails are captured for supporting any downstream audits of the projects by the finance or audit organization such as STQC.

f. Managed Services

The Departments should separately indicate the requirements for cloud services and for the Managed Services – Migration, Back Up, Disaster Recovery, Operations and Maintenance. This separation gives clarity on the responsibilities of the Managed Service Provider and of the Cloud Service Provider.

g. Pay-As-You-Go utility model

One of the key advantages of moving to cloud is the elasticity and ability to augment or decrease the resources (compute, memory, storage…) as required, to align with the performance requirements of the solution. Having the ability to scale up or scale down during the course of the project not only ensures optimal utilization of resources and standard performance (even during peak usage periods) but also alleviates the risk of under-sizing or oversizing the capacity requirements.

Therefore, the Department is required to move away from the traditional fixed payment model to a variable pricing / utility pricing model where the department pays for the resources it actually uses during that period. The payment terms have to be structured accordingly to pay only for the resources used by the department.

h. Evaluation of CSPs

The departments may choose the lowest commercial quote (L1) or adopt a QCBS evaluation as part of the commercials to procure the best fit solution for the department based on the project requirements.

i. Contractual Terms and Service Level Objectives

The departments need to be aware of certain critical issues when dealing with cloud contracts. Some of these issues will be similar to the information technology contracts, but even in respect to those issues, the nature of cloud computing can create new or different risks and departments may need to consider those issues such as Data Location, Legal Compliance, Security, Data Management during exit in the cloud computing context.

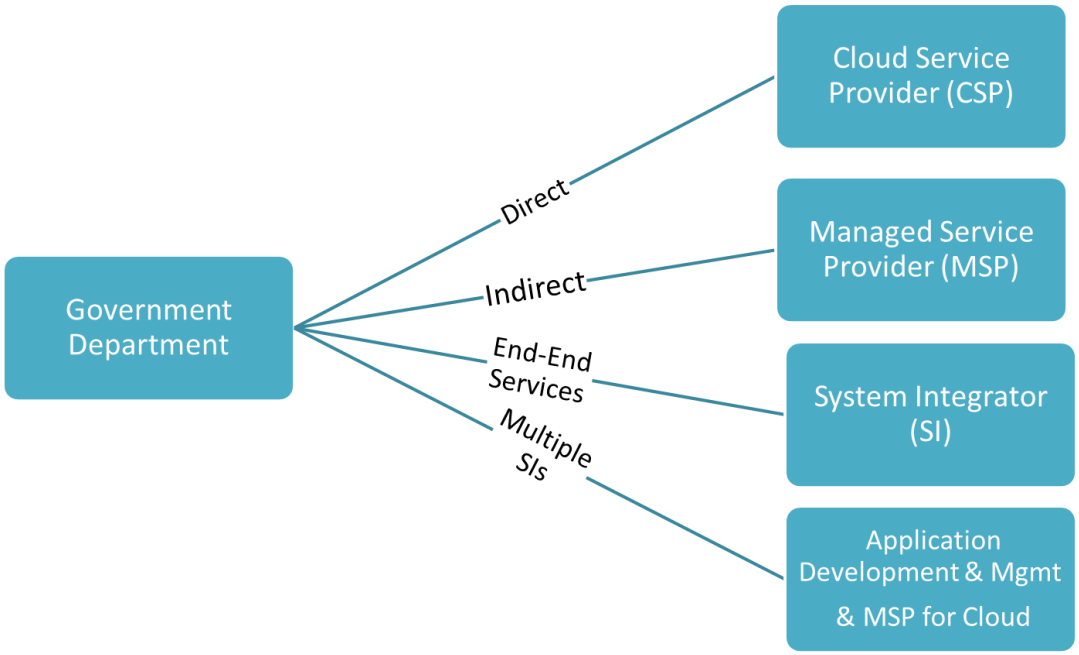
Cloud Service Level Agreements (Cloud SLAs) form an important component of the contractual relationship between a cloud service customer and a cloud service provider of a cloud service. There is a need to identify critical Service Levels for cloud (ex: timely service provisioning/de-provisioning) and also standardize the SLA terminologies across CSPs as the Service Level definition, measurement etc.

The guidelines on the contractual terms and the SLAs are prepared as separate documents.

The Government Department/Agency will invite bids for procuring the cloud services. The subsequent sections elucidate the details on the above mentioned components that can be used by the Departments when preparing the RFP.

3. Models for Engaging the Cloud Service Provider

There are multiple scenarios or engagement models for procuring cloud services as indicated below: The Government Department/ Agency may choose the right Scenario and accordingly specify the requirements in the RFP.



Scenario #1 (Self – Service Model): Procure Cloud Services directly from Cloud Service Provider (CSP): The Government Department / Agency have a suite of legacy applications and /or plans to implement new solutions. Government Department / Agency will procure cloud services directly from CSP when it already has in place an Implementing Agency or an Internal IT Team or expertise that is responsible for not only the implementation and operations of the Application Suite but also the underlying infrastructure. The department could also procure cloud services from re-sellers. The Government Department / Agency may consider migrating the existing application suite to Cloud and preparing an RFP to procure cloud service offerings. The Implementing Agency or the internal team will be responsible for migrating to cloud and managing the cloud service offerings along with the operations of the application suite. It is the responsibility of the Government Department / Agency to monitor the cloud services (Resource Management, User Administration, Performance, Service Levels…).

Scenario #2: Procure Cloud Services through a Managed Service Provider: The Government Department / Agency have a suite of legacy applications and /or plans to implement new solutions. Government Department / Agency have already identified an Application

Development Agency / Agencies as a partner agency that is responsible only for implementation and operations of the Application Suite. The Government Department / Agency intends to migrate the application suite to Cloud and is preparing an RFP to select cloud service offerings along with a Managed Service Provider (Some CSPs also provide MSP services), who will be responsible for migrating to cloud and managing the cloud service offerings. The application responsibilities will remain with the respective Application Development Agencies. It is the responsibility of the Managed Service Provider to monitor the cloud services (Resource Management, User Administration, Performance, Service Levels…).

Scenario #3 – Procurement of end-to-end services through a System Integrator: Government Department / Agency procures end-to-end services of which cloud services would be a part of the total services procured through a System Integrator (SI) for a turnkey project implementation. The underlying infrastructure is provided by SI and the SI is responsible for the performance of the application and its SLAs.

Scenario #4 - The Government Department / Agency may engage SI(s) for Application Development/Management and an MSP (Some CSPs also provide MSP services) to procure cloud services. The SI will be responsible for the Application SLAs and the MSP will be responsible for the Cloud SLAs. The Government Department / Agency will enter in to an agreement with each of them separately.

4. Key Components of Cloud Services

As explained in Section 2 above, the Departments may consider the following key components while procuring Cloud Services.

a. Cloud Services Requirements
b. Security – Shared Responsibility
c. Migration of Existing Systems to Cloud
d. Operational & Monitoring Requirements
e. Exit Management/Transitioning out services
f. Managed Services
g. Role of Government Departments
h. Pay-As-You-Go utility model
i. Evaluation of CSPs
j. Contractual Terms and Service Level Objectives

The detailed requirements of each of the above components are provided in the following sections. While the requirements are provided to enable Departments to prepare the RFP, the responsibility of implementation on behalf of the department lies with the MSP or SI, as the case may be, and not necessarily the department.

4.1 Cloud Services Requirements

The indicative requirements for cloud services are given below:

a. Environment to be set up

b. The Service model Requirements

c. Defining the Requirements for Cloud Services

d. Details of Existing Software Licenses

e. Additional Requirements specific to a project

f. CSP Support Requirements

a. Environment to be set up

The Government Department/Agency shall indicate the requirement of the following environments based on the project requirements along with the choice of the deployment model public / virtual private / government community .

- Pre – Production: The department may plan for the following sub-environments based on the project requirements.
    - Development / Test
    - Quality / Staging
    - Training

Departments may indicate a minimum requirement for example - 15% of the production requirements with the flexibility to scale up or scale down or the same can be re-allocated to the pre-production (from development to testing etc.) or to production environment based on the requirements

- Production
- Disaster Recovery

The environments (public / virtual private / government community) shall comply with the respective Provisional Empanelment Compliance Requirements.

b. The Service model Requirements

Based on the project requirements the Government Department may choose to procure one/some of the following Service Model empanelled by MeitY and indicate any additional requirements over and above the requirements mentioned in the Provisional Empanelment Compliance Requirements.

I. Infrastructure as a Service (IaaS) Requirements
II. Platform as a Service (PaaS) Requirements
III. Disaster Recovery as a Service
IV. Virtual Desktop as a Service (VDaaS) Requirements
V. DevOps as a Service (DevOps) Requirements

The department may indicate the requirements for each of the service model as indicated in Annexure 2.

c. Defining the Requirements for Cloud Services

The Government Department/Agency need to estimate the resources required on cloud based on the application, workload etc. There are also a variety of tools and resources available with the CSPs to estimate the resources on cloud based on the current / anticipated server, storage configurations and workloads. The Government Department / Agency may utilize such tools along with the envisaged TO BE architecture to arrive at the estimates for the Day One Operating Environment. The department can indicate the requirements for both – legacy as well new application deployment to cloud.

The Government Department/Agency may indicate the requirements in either of the formats provided below. The Department may choose Model #1-Indicative Requirements if the workloads are unpredictable (this model may result in high costs as an on-demand pricing is offered) or may choose Model #2 if the Department can estimate/predict the minimum workloads. (As some minimum quantity is assured or committed by the department some CSPs offer a discounted price).

The indicative or the minimum requirements need to be provided for each kind of environment (Development, QA, Training, Staging, and Production - as applicable for the project) that is planned on cloud.

Model #1: Indicative Requirements along with Indicative projections for subsequent years with the flexibility to scale up or scale down as per the actual workloads

S. No.	Description	Unit of Measurement for Pricing	Multiplication Factor[1]	Indicative Projections		
		(1)	(3)	Year1	Year2	Year 3
	Virtual Machines (*In case of requirement of VMs of different configuration, include individual line items providing the VM configuration (type of VM, number of virtual CPUs / cores, Speed, memory, storage,)*					
1.	Example: 2*4*20	Per Hour	Example: 1000 hours Or 3*365 x 24 hours [Years*days*hours]			
2.	**……**					
	Storage - *In case of requirement of Storage of different configuration, include individual line items providing the Storage configuration details*					
3.	*Example : 512*	per GB per Month	Example: 512/month for 12 months - 512*12*3			
4.	**…..**					
5.	**Throughput**	per GB per Month				
	Other Cloud Services (e.g., ELB, PaaS…). Include individual line items as required for each of the Cloud Services					
6.	**ELB**	Put an appropriate unit on which price is calculated	Put an appropriate multiplication factor that makes the figure significant for price comparison			
7.	**…..**					
	Additional Services - Include individual line items as required for each of the Services that are required to be implemented to meet the RFP requirements and that have commercial implications					
8.	**Load Balancing**	Put an appropriate unit on which price is calculated	Put an appropriate multiplication factor that makes the figure significant for price comparison			

. No.	Description	Unit of Measurement for Pricing	Multiplication Factor[1]	Indicative Projections		
		(1)	(3)	Year1	Year2	Year 3
9.	**VLANs**	Put an appropriate unit on which price is calculated	Put an appropriate multiplication factor that makes the figure significant for price comparison			
10.	**…..**					
11.	**Any other tools required**					

Note: 1. The Multiplication factor is used to arrive at a cost that would be a significant component in the commercial evaluation along with other costs such as Migration, O&M etc.

The above are only indicative requirements and are provided with the explicit understanding that during the duration of the contract these nominal requirements will change. The Service Provider shall continue to develop and refine infrastructure in accordance with emerging requirements and evolving technology specifications as required. Refer to Annexure 1 for the possible assessment to be carried out by the Government Department/Agency to arrive at the Day One Operating Environment for Complex Legacy Environment.

Model #2: Minimum assured requirement defined year-on-year with the flexibility to scale up to meet the peak workloads

*(Under this model, the price quoted will be applicable till the minimum/committed resources are consumed - for example: say if the department commits 10 VMs for 24 hours for 365 days and if it uses 12 VMs in the first month then the then the rate quoted will be applicable to the 12 VMs (not just for 10 VMs) – 12*24*30 hours. After the total number of hours - 10* 24*365 are consumed, the additional resources will be charged based on the on-demand price quoted by the bidder or the CSP.)*

. No.	Description	Unit of Measurement for Pricing	Quantity	Multiplication Factor*	Minimum Requirement		
					Year1	Year2	Year 3
	Virtual Machines (*In case of requirement of VMs of different configuration, include individual line items providing the VM configuration (type of VM, number of virtual CPUs / cores, Speed, memory, storage,)*						
1.	Example: 2*4*20	Per Hour	Example: 4	Example: 4*24*365*3 hours [quantity*hours in a day*days in a year*no. of years] Or (Indicate total no. of hours)			
2.	**……**						
	Storage - *In case of requirement of Storage of different configuration, include individual line items providing the Storage configuration details*						
3.	*Example : 256*	per GB per Month	Example: 512/month	Example: 512*12*3 [GB*months*years]			
4.	**…..**						
5.	**Throughput**	per GB per Month	Example: 10 GB/month	Example: 10*12*3 [GB*months*years]			
	Other Cloud Services (e.g., ELB, PaaS…). Include individual line items as required for each of the Cloud Services						
6.	**ELB**	Put an appropriate unit on which price is calculated		Put an appropriate multiplication factor that makes the figure significant for price comparison			
7.	**…..**						
	Additional Services - Include individual line items as required for each of the Services that are required to be implemented to meet the RFP requirements and that have commercial implications						
8.	**Load Balancing**	Put an appropriate unit on which price is calculated		Put an appropriate multiplication factor that makes the figure significant for price comparison			

. No.	Description	Unit of Measurement for Pricing	Quantity	Multiplication Factor*	Minimum Requirement		
					Year1	Year2	Year 3
9.	**VLANs**	Put an appropriate unit on which price is calculated		Put an appropriate multiplication factor that makes the figure significant for price comparison			
10.	**…..**						
11.	**Any other tools required**						

d. Software Licenses

i. If The Government Department / Agency has already procured or has existing software licenses that it intends to deploy and continue using on the cloud then a table listing out the inventory of the existing software licenses (OS, DB …) need to be provided for consideration for the Managed Service Provider /SI to assess for deployment on the Cloud environment from a Technical and Commercial perspective**.** The Department may also assess if any upgrades are required for the existing licenses (to the latest versions) and the details of such requirements may be indicated in the table.

ii. In case of new projects where the departments need to procure software licenses, the departments may consider procuring them as part of Platform-as-a-Service (PaaS). The department initially may procure the minimum required licenses and later based on the work load can procure additional licenses if required.

e. Additional Requirements

These are additional requirements in addition to the requirements published by Meity in the RFP for Provisional Empanelment Compliance by the CSPs.

a. Additional Security Requirements (e.g., PCI – DSS, Data Encryption, Third Party Authentication Support, …) as per the requirements of the data handled by the Government Department / Agency

b. Auto Scaling Limit

c. Data Retrieval Period (length of time in which the customer can retrieve a copy of their cloud service customer data from the cloud service):

d. Data retention period (length of time which the cloud service provider will retain backup copies of the cloud service customer data during the termination process (in case of problems with the retrieval process or for legal purposes). Residual data retention (refers to a description of any data relating to the cloud service customer which is retained after the end of the termination process – typically this will be cloud service derived data, which could be subject to regulatory controls):

e. Log Access Availability (what log file entries the cloud service customer has access to)

f. Logs retention period (the period of time during which logs are available for analysis)

g. Backup Requirements (Departments should indicate the estimated size of data)

    i. Data Mirroring Latency (the difference between the time data is placed on primary storage and the time the same data is placed on mirrored storage)

    ii. Data Backup Method (list of method(s) used to backup cloud service customer data):

    iii. Data Backup Frequency (the period of time between complete backups of data)

    iv. Backup Retention Time (the period of time a given backup is available for use in data restoration)

    v. Backup Generations (the number of backup generations available for use in data restoration)

    vi. Maximum Data Restoration time (the committed time taken to restore cloud service customer data from a backup)

h. Provide support for automation tools for data portability

i. Data portability format (the electronic format(s) in which cloud service customer data can be transferred to/accessed from the cloud service)

j. Data portability interface (the mechanisms which can be used to transfer cloud service customer data to and from the cloud service. This specification potentially includes the specification of transport protocols and the specification of APIs or of any other mechanism that is supported)

k. Data transfer rate (refers to the minimum rate at which cloud service customer data can be transferred to/from the cloud service using the mechanism(s) stated in the data interface)

l. Platform migration (P series / SPARC to X86), OS migration requirements may be indicated if required for the project.

f. CSP Support Requirements

CSPs provide multiple support options catering to the varying levels of support requirements (e.g., access to customer service, documentation, forums, technical assistance) for its customers. Appropriate support at the right stage of the project (e.g., Migration, Go-Live...) may be sought from the CSP as part of the RFP.

4.2 Security – Shared Responsibility

The CSP and the departments share control over the Cloud environment and therefore both parties have responsibility for managing it. The CSP's part in this shared responsibility includes providing its services on a highly secure and controlled platform and providing a wide array of security features customers can use. The departments' responsibility includes configuring their IT environments in a secure and controlled manner for their purposes.

Infrastructure services: The CSP manages the security of Facilities, Physical security of hardware , Network infrastructure and Virtualization infrastructure while the department is responsible for the security of the Virtual Machine Images, Operating systems, Applications, Data in transit, Data at rest, Data stores, Credentials and Policies and configuration. The department can implement encryption of data at rest, or HTTPS encapsulation for the payloads for protecting the data in transit to and from the service.

Platform services: The CSPs manage the underlying infrastructure and foundation services, the operating system and the application platform. The CSP platform may provide data backup and recovery tools; but it is the responsibility of the department to configure and use tools in relation to the project requirements - business continuity and disaster recovery (BC/DR) policy. The department will be responsible for the data and for firewall rules for access to the platform/container services. For example the CSP may provide security groups and allow the department to manage firewall rules through the CSPs security groups for the instances.

Some of the security tools offered by CSPs and other third party vendors include:

- Identity and Access Management (IAM) - allows controlling the level of access to the users to the CSPs infrastructure services. With IAM, each user can have unique security credentials, eliminating the need for shared passwords or keys and allowing the security best practices of role separation and least privilege.
- Secure Access – Customer access points, also called API endpoints, allow secure HTTP access (HTTPS) so that the departments can establish secure communication

sessions with Cloud services using Secure Sockets Layer (SSL)/Transport Layer Security (TLS).

- Built-in Firewalls – can control how accessible the instances are by configuring built-in firewall rules
- Multi-Factor Authentication (MFA), Encrypted Data Storage, Centralized Key Management, DDoS Protection (safeguards web applications running on cloud)
- Additional third-party security products for network security, server and end point protection and vulnerability management as per the security requirements of the specific project.

While the security tools are provided by the CSP, it is the department's responsibility (the MSP or the SI as the case may be) to implement and configure them based on the project requirements.

Departments also need to ensure that the CSPs facilities/services are certified to be compliant to the following standards:

- ISO 27001 - Data Center and the cloud services should be certified for the latest version of the standards
- ISO/IEC 27017:2015-Code of practice for information security controls based on ISO/IEC 27002 for cloud services and Information technology
- ISO 27018 - Code of practice for protection of personally identifiable information (PII) in public clouds.
- ISO 20000-9-Guidance on the application of ISO/IEC 20000-1 to cloud services
- PCI DSS - compliant technology infrastructure for storing, processing, and transmitting credit card information in the cloud,

Meity with the help of STQC is carrying out the audit and is in the process of certifying the service offerings of CSPs for the above three standards.

4.3 Migration of existing applications

The following activities are to be undertaken if the department has legacy applications (full suite or partial) that are planned to be migrated to cloud.

a. Migration Planning: Comprehensive planning for migration of the application suite and data to the cloud including developing the migration roadmap identifying the constraints and inhibitors to cloud migration. The migration plan should detail out:

i. The configuration proposed to fulfill day-1 requirements with the explicit understanding that during the duration of the contract these nominal profile requirements will change

ii. Procedures and documentation to be developed for migration of applications and data & content including redevelopment/additional development that may be required

iii. Plans for co-existence of non-cloud and cloud architectures during and after migration

iv. Communication, change management, and training needs

v. Cloud governance for post-implementation

vi. Test Plans for verifying successful migration

vii. Detailed Risk Management Plan that will identify potential risks, set out possible mitigation approaches, and identifies specific tasks the Service Provider will undertake to help avoid identified risks connected with the Migration.

b. Migration

i. Changes to the applications based on:

1. Complete architectural understanding of the existing applications and processes necessary for successful migration of the applications and data as well as continued operation and maintenance of the services

2. Analysis of the interdependencies such as application dependencies and affinities to servers, server configuration etc.

3. Dependencies between applications and data

ii. Provision the necessary compute & storage infrastructure on the cloud including the underlying software licenses to host the Application Suite that meet or exceed the day-1 minimum capacity

iii. Setup of *Development, Quality, Production and Disaster Recovery* Environments by provisioning the necessary compute & storage infrastructure on the cloud along with the underlying software licenses to host the Application Suite.

iv. Configuring external connections to the hosted infrastructure required to upload database backups and virtual machine (VM) images to the hosting environment.

v. Migration of the Application Suite from the existing infrastructure to the cloud infrastructure. The migration (supported by SI) shall also include the migration of

underlying data & files from the current database(s) / storage into the database(s) / storage on the cloud.

vi. To enable easy migration to cloud, Department may consider up-gradation of OS & DB to latest version available in market.

vii. Deployment of the new Applications on the cloud environment as per the TO BE Architecture.

viii. Configure, manage, deploy, and scale the system on environments setup on cloud

c. Managing and Monitoring Migration

i. Manage (including project managing), coordinating and planning all aspects of migration

ii. Proactively identify, monitor and manage any significant risks or issues in relation to migration

iii. Provide regular progress reports to the Government Department / Agency

1. A listing of all Migration Deliverables and Milestones, including acceptance status, the estimated time to completion, days overdue, planned completion date, and actual completion date and comments, as well as a report identifying the status of all Milestones (for example: red, amber, green)

2. A listing of all unresolved issues related to the execution of the Migration Plan, along with due dates, priority, responsible party, and an assessment of the potential and actual business impact and impact to the Migration Plan

3. Status of the any risks, including those identified in the Risk Management Plan, as well as the steps being taken to mitigate such risks

4.4 Operation and Maintenance

Deployment on cloud requires continuous monitoring and management. Migrating to cloud creates a model of shared responsibility between the Government Department / Agency and the Cloud Service Provider.

The operations and maintenance of the infrastructure including host operating system and virtualization layer down to the physical security of the facilities in which the service operates will be the responsibility of the Cloud Service Provider. The Government Department / Agency has the responsibility for the management of the guest operating

system (including updates and security patches), other associated application software, and the configuration and management of the security solutions provided by Cloud Service Provider such as security groups, host-based firewalls, host-based intrusion detection/prevention, encryption, and key management solutions.

The responsibility of operating the IT environment including management, operation, and verification of shared IT controls is shared between the Government Department / Agency and Cloud Service Provider. While the CSP manages those controls associated with the physical infrastructure deployed in the cloud environment, the Government Department / Agency is responsible for using the CSP control and compliance documentation (e.g., CSP self-certifications and Third-party Certifications) to perform their control evaluation and verification procedures as required.

The Government Department / Agency may choose to procure the following managed services (O&M – Cloud Services) from a Managed Service Provider (MSP) in addition to the Cloud Services to handhold the department in managing the operations on the cloud.

a. Resource Management

i. Adequately size the necessary compute, memory, and storage required, building the redundancy into the architecture (including storage) and load balancing to meet the service levels (cloud services) mentioned in the RFP and the application service levels.

ii. While the initial sizing & provisioning of the underlying infrastructure (including the system software and bandwidth) may be carried out based on the information provided in the RFP, subsequently, it is expected that the Service Provider, based on the growth in the user load (peak and non-peak periods; year-on-year increase), will scale up or scale down the compute, memory, storage, and bandwidth requirements to support the scalability and performance requirements of the solution and meet the SLAs.

iii. 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.

iv. The scaling up / scaling down (beyond the auto-scaling limits or whenever the auto-scaling limits have to be changed) has to be carried out with prior approval by the Government Department / Agency. The Service Provider shall provide the necessary details including the sizing calculations, assumptions, current

workloads & utilizations, expected growth / demand and any other details justifying the request to scale up or scale down.

v. Manage the instances of storage, compute instances, and network environments. This includes department-owned & installed operating systems and other system software that are outside of the authorization boundary of the CSP. Service Provider is also responsible for managing specific controls relating to shared touch points within the security authorization boundary, such as establishing customized security control solutions. Examples include, but are not limited to, configuration and patch management, vulnerability scanning, disaster recovery, and protecting data in transit and at rest, host firewall management, managing credentials, identity and access management, and managing network configurations.

vi. Provisioning and configuring their implementation of storage, virtual machines, and VPCs that allows for the Service Provider to launch and terminate cloud instances, change firewall parameters, and perform other management functions. Upon deployment of virtual machines, the Service Provider has to assume full administrator access and is responsible for performing additional configuration, patching, security hardening, vulnerability scanning, and application installation, as necessary.

vii. For the underlying system software (procured under platform as a service), the Service Provider shall provide the Annual Technical Support (ATS) from the OEM during the entire period of the contract.

b. User Administration

i. Implement Identity and Access Management (IAM) that properly separates users by their identified roles and responsibilities, thereby establishing least privilege and ensuring that users have only the permissions necessary to perform their assigned tasks. *(Only relevant if IAM is getting implemented)*

ii. Administration of users, identities and authorizations, properly managing the root account, as well as any Identity and Access Management (IAM) users, groups and roles they associated with the user account.

iii. Implement multi-factor authentication (MFA) for the root account, as well as any privileged Identity and Access Management accounts associated with it.

c. Security Administration and monitoring Security Incidents

i. Appropriately configure the security groups in accordance with the Government Department / Agency's networking policies

ii. Regularly review the security group configuration and instance assignment in order to maintain a secure baseline.

iii. Secure and appropriately segregate / isolate data traffic/application by functionality using DMZs, subnets etc.

iv. Ensure that the cloud infrastructure and all systems hosted on it, respectively, are properly monitored for unauthorized activity.

v. Properly implementing anti-malware and host-based intrusion detection systems on their instances, as well as any required network-based intrusion detection systems in accordance with the Government Department / Agency's policies.

vi. Conducting regular vulnerability scanning and penetration testing of the systems, as mandated by their Government Department / Agency's policies.

vii. Review the audit logs to identify any unauthorized access to the government agency's systems.

d. Monitoring Performance and Service Levels (Availability, Incident Management, Performance)

i. Provide and implement tools and processes for monitoring the availability of assigned applications, responding to system outages with troubleshooting activities designed to identify and mitigate operational issues.

ii. Reviewing the service level reports, monitoring the service levels and identifying any deviations from the agreed service levels

iii. Independent monitoring of service levels, including availability, uptime, performance, application specific parameters, e.g. for triggering elasticity, request rates, number of users connected to a service

iv. Receiving and processing service level reports from the cloud service provider (or a trusted third party (auditor), comparing them with SLA objectives.

v. Detecting and reporting service level agreement infringements

vi. Responding to SLA infringements either as reports from the cloud service provider or detected by Service Provider or Government Department / Agency (for example, informing their end-users of service interruptions, raising a ticket, claiming service credits etc.)

vii. Resolving disputes around SLA infringements

viii. Provide and document patch management appropriate to all components within the cloud service provider's boundary and to adhere to Government Department/Agency or MietY standards, if any.

ix. Monitoring of performance, resource utilization and other events such as failure of service, degraded service, availability of the network, storage, database systems, operating Systems, applications, including API access within the cloud service provider's boundary.

e. Backup

i. Formulate a Backup Policy

1. Files & Images: Frequency for full backups and incremental backups
2. Databases and log files: Frequency for full backups and incremental backups
3. Off-site backup requirement that still meets the prescribed RTO requirements>
4. Restoration timeline requirements: e.g., initiate a minimum of 95 percent << this may be changed as per the project requirements >> 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
5. Files & Images: Retention timelines of inactive versions of the backups
6. Databases & log files: Retention timelines of inactive versions of the backups
7. Preservation and Retention of Data [required for certain domain specific projects]

ii. Configure, schedule, monitor and manage backups of all the data including but not limited to files, images and databases as per the policy finalized by Government Department / Agency.

iii. Administration, tuning, optimization, planning, maintenance, and operations management for backup and restore;

iv. Provision capacity for backup and restore, as required

v. Perform backup on the next scheduled backup window in case of any scheduling conflicts between backup and patch management.

vi. Specific Snapshot Objective – At the Government Department / Agency's request, the Service Provider shall create a full snapshots for the platform, content and related data, to be retrieved at the Component Agency's request within 24 hours up to a period to be determined by the Component Agency

f. Usage Reporting and Billing Management

i. Track system usage and usage reports

ii. Monitoring, managing and administering the monetary terms of SLAs and other billing related aspects.

iii. Provide the relevant reports including real time as well as past data/information/reports for the Government Department / Agency to validate the billing and SLA related penalties

4.5 Exit Management / Transition-Out Services

The responsibilities include:

a. Migration of the VMs, data, content and any other assets to the new environment or on alternate cloud service provider's offerings and ensuring successful deployment and running of the Government Department's solution on the new infrastructure by suitably retrieving all data, scripts, software, virtual machine images, and so forth to enable mirroring or copying to Department supplied industry standard media.

b. The format of the data transmitted from the cloud service provider to the Department should leverage standard data formats (e.g., OVF, VHD…) whenever possible to ease and enhance portability.

c. 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 / Agency.

d. Ensure that all the documentation required for smooth transition including configuration documents are kept up to date

e. Ensure that the CSP does 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 / Agency. If data is to be retained the cost for retaining the data may be obtained in the commercial quote.

f. Once the exit process is completed, remove the data, content and other assets from the cloud environment and destroy the VM, Content and data of the Government Department / Agency as per stipulations and shall ensure that the data cannot be forensically recovered.

4.6 Managed Services

The departments can procure Disaster Recovery, Exit Management Services, Operations & Management Services, Migration and Provisioning Services, Back up and Support Third Party Audit and other requirements as a Managed Service.

The following sections indicate certain responsibilities specific to the Managed Service Provider or a System Integrator. The responsibilities indicated below for (Disaster Recovery, Exit Management Services, Operations and Management Services, Support for Third Part Audit) along with the requirements indicated in the above sections may be included in the RFP when defining the scope of services for the MSP.

a. Disaster Recovery

The following requirements may be included as responsibilities of the MSP in the RFP:

i. In addition to the production environment, the MSP is responsible for Disaster Recovery Environment and the associated services so as ensure continuity of operations in the event of failure production environment and meet the RPO and RTO requirements. However, during the change from DC to DRC or vice-versa (regular planned changes) there should not be any data loss.

ii. Sizing and providing the DC-DR replication link so as to meet the RTO and the RPO requirements.

iii. Conduct DR drill for two days (for the Department's environment) 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 and should meet the RTO and RPO requirements. The Service Provider shall clearly define the procedure for announcing DR based on the proposed DR solution. The Service Provider 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 Service Provider shall plan all the activities to be carried out during the Disaster Trial and issue a notice to the Government Department/Agency at least two weeks before such trial.

b. Exit Management Services

The following requirements may be included as responsibilities of the MSP in the RFP:

i. Provide a comprehensive exit management plan.

ii. Carry out the migration of the VMs, data, content and any other assets to the new environment created by the Government Department / Agency or any other Agency (on behalf of the Department) on alternate cloud service provider's offerings to enable successful deployment and running of the Government Department's solution on the new infrastructure.

iii. Address and rectify the problems with respect to migration of the *Government Department / Agency* application and related IT infrastructure during the transition.

iv. Ensure that all the documentation required by the Government Department / Agency for smooth transition (in addition to the documentation provided by the Cloud Service Provider) are kept up to date and all such documentation is handed over to the Government Department / Agency during regular intervals as well as during the exit management process.

v. Support and assist the Government Department / Agency for a period of Please Insert duration so that l the Government Department / Agency is able to successfully deploy and access the services from the new environment.

vi. Train and transfer the knowledge to the Replacement Agency (or Government Department / Agency) to ensure similar continuity and performance of the Services post expiry of the Agreement.

c. Operation and Maintenance Services

i. Advise the Government Department / Agency on optimal operational practices, recommend deployment architectures for cloud infrastructures, design and implement automated scaling processes, day-to-day and emergency procedures, deploy and monitor underlying cloud services, performance reporting and metrics, and ensure the overall reliability and responsive operation of the underlying cloud services through both proactive planning and rapid situational response.

ii. Interface with the Cloud Service Provider(s) on behalf of the Government Department / Agency for all activities including monitoring the reports (e.g., usage, security, SLA,), raising (or escalating) tickets / incidents and tracking the same to resolution.

iii. Prepare a comprehensive O&M plan for managing the cloud services and keep it updated with any changes during the course of the project.

iv. Create and maintain all the necessary technical documentation, design documents, standard operating procedures, configurations required to continued operations and maintenance of cloud services.

d. Support Third Party Audit and other requirements (e.g., Forensic Investigations...)

Support the third party auditor / program management team / internal IT team with respect to third party audits and other requirements such as forensic investigations, SLA validation…

4.7 Payment Terms

1. Payment Schedules and Milestones

The payment terms have to be structured accordingly to pay only for the resources used by the department as indicated below:

Following payment milestones shall be applicable for the Cloud Services Consumed:

S. No.	Phase	Milestone	Amount
1	Monthly Payments *(The first monthly payment will be due on completion of one months from the Effective Date of Contract)*	At the end of each month after satisfactory delivery of the services. The final payment will be made on successful completion of transition.	Payment will be based on the actual usage of the services and as per the "Unit Costs" under Pricing Summary Sheet

Below additional payment terms are indicated in case department is procuring managed services

Following payment milestones shall be applicable for the Managed Services delivered:

S. No.	Phase	Milestone	Amount
1	Mobilization Advance *(The* Government *Department / Agency may choose whether or not to pay the mobilization advance based on the requirements. If it chooses not to pay the advance then the Advance Bank Guarantee would not be*	On Signing of Contract and Fulfillment of Conditions Precedent including Submission of Advance Bank Guarantee of Equal Amount	0 to 30% of Cost Quoted for Migration (Refer to "Migration and Provisioning Services" Cost Quoted under the Pricing Summary Sheet.

	required. Usually 10% is paid as mobilization advance, however a higher mobilization advance may be considered in complex Migration Projects that require migration tools - proprietary tools and Accelerators - to be deployed for a Migration		
2	Successful Completion of Migration	Successful Migration of existing system to Cloud Environment and sign-off from the Government Department / Agency	70% to 100% of Cost Quoted for Migration and Provisioning (Refer to "Migration and Provisioning Services" Cost Quoted under the Pricing Summary Sheet.
3	Operations & Maintenance Costs - Monthly Payments *(The first monthly payment will be due on completion of one month from the Date of Successful Completion of Migration)*	At the end of each Month after satisfactory delivery of the services. The final O&M payment will be made on successful completion of transition.	Equated Monthly Installments EMI-I calculated from the "Operations and Maintenance – Cloud Services Cost for a period of 2 Years" for the first 36 months. EMI-II calculated from the "Operations and Maintenance – Cloud Services Cost for the extended optional 1 Year" for the remaining 12 months.

Payment for Cloud Services

1. Monthly Payment to be based on the actual usage of the services and as per the "Unit Costs" under Pricing Summary Sheet

2. Total Monthly Payment to be linked to the compliance with the SLA metrics and the actual payment is the payment due to the Service Provider after any SLA related deductions.

3. Setup Costs (Refer to the "Cloud Services – Setup Costs" under Pricing Summary Sheet) will be paid along with the First Month Payment.

Payment for Managed Services:

4. EMI to be made at the end of the month after satisfactory delivery of the services

5. Total Monthly Payment should be linked to the compliance with the SLA metrics and the actual payment is the payment due to the Service Provider after any SLA related deductions.

6. **Additional Services:** Government Department / Agency have the option to avail the additional services of Service Provider for carrying out any extension or changes in services, as a part of the project. All such additional services will be initiated using the Change Control Procedures that will be defined in the Agreement. The unit costs, where available, quoted in the commercial proposal will be used for such approved additional work.

Payments If SI is engaged to provide end to end services:

7. In a scenario where the SI is engaged to provide end to end services, the cloud services could be one component amongst several other solution components that includes application development, training etc. The following payment options may be considered:

    - The Department may ask the SI to quote the commercials for cloud in the formats indicated in Annexure 3. However in order to ensure that the SI does not under-size the requirements, Departments may validate/evaluate the Technical BoM during the technical evaluation.

    - Alternatively, the SI may be asked to quote a consolidated amount for the cloud services (with a break-up for each year) along with the Technical Bill of Materials (BoM). A fixed Payment (Equated Monthly or Quarterly Instalment) to SI may be made for cloud services as is usually done in traditional procurement. However, in this case, the Department will not be leveraging the advantage of paying for the resources that it actually consumes or utilizes.

4.8 Role of Government Departments in Operations Phase

It is essential that the Department monitors the operational activities to ascertain that the MSP/SI has implemented the cloud features mentioned in the RFP. The Departments need to review and validate the security configurations created by the MSP, review the notifications and patches released by the CSP and validate that the same is being taken into consideration by the MSP during operations, confirm that the audit trails (e.g., who is accessing the services, changes to the configurations, etc.) are captured for supporting any downstream audits of the projects by the finance or audit organization such as STQC.

The departments may ensure that the MSP/SI implements tools/services that provide the following features (indicative) to enable departments to monitor the performance, security, resource utilization etc.

- View into the performance and availability of the cloud services being used, as well as alerts that are automatically triggered by changes in the health of those services.
- Receive alerts that provide proactive notifications of scheduled activities, such as any changes to the provisioned cloud resources.
- System-wide visibility into resource utilization, application performance, and operational health through monitoring of the cloud resources.
- Review of auto-scaling rules and limits.
- Access to Logs of all user activity within an account. The recorded information should include API details. This is required to enable security analysis, resource change tracking, and compliance auditing.
- Ability to discover all of the provisioned resources and view the configuration of each. Notifications should be triggered on configuration changes, and departments should be given the ability to view the configuration history to perform incident analysis.
- Monitoring of cloud resources with alerts to customers on any security configuration gaps.

4.9 Evaluation Process

The departments may choose the lowest commercial quote (L1) or adopt a QCBS evaluation as part of the commercials to procure the best fit solution for the department based on the project requirements. Departments may follow General Financial Rules (GFR) 2017.

The departments based on the project requirements may include functional specifications in the RFP and evaluate the offered cloud solution against the compliance to the functional specifications. In addition to the compliance to the functional specifications, it may consider to have a Proof of Capability (PoC) as part of the technical evaluation to demonstrate the key features such as auto-scaling, security controls, management & administration, logging and auditing capabilities of the offered cloud solution. In such a scenario the departments may adopt a QCBS evaluation as part of the commercials to procure the best fit solution for the department.

The Commercial bid formats are given in Annexure-3.

4.10 Contractual Terms and Service Level Objectives

The departments need to be aware of certain critical issues when dealing with cloud contracts. Some of these issues will be similar to the information technology contracts, but even in respect to those issues, the nature of cloud computing can create new or different risks and departments may need to consider those issues such as Data Location, Legal Compliance, Security, Data Management during exit in the cloud computing context.

Cloud Service Level Agreements (Cloud SLAs) form an important component of the contractual relationship between a cloud service customer and a cloud service provider of a cloud service. There is a need to identify critical Service Levels for cloud (ex: timely service provisioning/de-provisioning) and also standardize the SLA terminologies across CSPs as the Service Level definition, measurement etc.

The guidelines on the contractual terms and the SLAs are available as separate documents.

Annexure 1 – Guidelines for Legacy Applications Migration

Guidelines for Legacy Applications Migration

The Government Department / Agency is expected to carry out the below tasks to determine the current inventory, assess the current environment to determine which workloads and applications are suitable for migration, determining the service and deployment models, developing the business case and TO-BE architecture as pre-requisite for preparing the RFP .

a. **Inventory of Users, Applications, Infrastructure, Security & Privacy, Service Management (applicable where there are legacy applications proposed to be migrated to cloud)**

   i. Inventory of IT assets to provide a comprehensive view of Government Department / Agency applications, infrastructure and security.

   ii. Analysis to identify the IT users and stakeholders that would be impacted by cloud migration.

   iii. Identified the business processes and governance processes that are associated with current inventory (both applications & infrastructure).

   iv. Formulated a baseline of Government Department / Agency's technical environment including inventory of both infrastructure and applications, to include development/testing environments.

   v. The functional and technical details of the applications including the stakeholders, functional architecture, technical architecture, integration with external solutions, underlying technologies / platforms, underlying software,….

   vi. The logical and physical deployment architectures including the below details:

      i. Physical Servers: Provide for each of the physical server: Application / Component; No. of Processors per server; No. of cores per processor; No. of Servers; Memory; Host (OS); Server Utilization (%) (Average hours per day each server is running and Average days per week each server is running)

ii. Provide for each of the Applications: Application / Component; No. of VMs; No. of CPU cores; Memory; Guest (OS); Hypervisor; VM Usage (%)

vii. The list of batch process

viii. The current utilizations (compute, storage, and network) and current & anticipated workloads of the application suite

ix. The security and privacy requirements currently implemented

x. The service management / operations & maintenance requirements

b. Application Profiling and Mapping identifying the Service Model (IaaS, PaaS, DRaaS, DevOps, VDaaS) and Deployment Model (Public, Virtual Private Cloud, Government Community Cloud) for the various applications (legacy and / or new) planned to leverage cloud services

i. Analysis of the interdependencies such as application dependencies and affinities to servers, server configuration etc.

ii. Identify and document critical dependencies between applications and data

iii. Understanding of the implications of moving individual applications or groups of applications to the cloud.

iv. Decomposition of applications & identification of common functions and services that can potentially be migrated to the cloud, and identification of potential shared services.

v. Comprehensive analysis and understanding of the current environment, that incorporates considerations for security such as data sensitivity, legal or other regulatory issues, disaster recovery and analysis of which on-premise technical resources / applications are best suited for the cloud

vi. Suitability analysis to identify appropriate service models (e.g. SaaS, PaaS, IaaS) and deployment models (e.g. private, public, hybrid, community)]

c. TO BE Architecture defining requirements such as

i. Pre-production, production, disaster recovery environments to be setup

ii. Various sub-nets to be setup logically isolating the pre-production and production environments as well as the public / internet facing components (DMZ) from the higher security backend components and databases

iii. Requirement of integration of the solutions on cloud with on-premise or external agency solutions

iv. Storage Architecture (mix of file, block, low-cost storage)

v. Requirement with respect to Load Balancers, VPN, and Auto-scaling limits…

vi. Requirements of additional security features such as Web Application Firewall…

vii. Any additional government-wide and Government Department / Agency - specific security controls (e.g., Encryption, PCI-DSS,..) required

viii. Disaster Recovery Environment Requirements along with the RPO / RTO requirements

ix. Backup & Archival Requirements

x. In case of a hybrid model, where the Government Department / Agency plans to use the existing infrastructure along with the cloud services, the same needs to be detailed in the TO BE architecture.

This page is intentionally left blank

Annexure 2 – Service Model Requirements

I. Infrastructure as a Service (IaaS) Requirements

The below requirements are in addition to the requirements published by MeitY in the Provisional Empanelment Compliance Requirements.

a. Pre-Production and Production Environment Requirements

Each of the environments, (Development / Test, Quality / Staging, and Training) should be logically isolated, i.e., separate from the production environment in a different VLAN than the production environment and setup such that users of the environments are in separate networks (e.g., development environment logically isolated from the other pre-production and production environments; Test & QA environment logically isolated from the other pre-production and production environments; Staging, and Training environment logically isolated from the other pre-production and production environments)

i. A change release management and configuration management procedure is defined and implemented to process any change to the cloud environment / services. This procedure must include the capability to support the transition between the aforementioned environments prior to production deployment.

b. Disaster Recovery Environment (indicative list below)

i. Geographical Location of the Disaster Recovery Environment (e.g., different seismic zone from the production environment or at a different place other than the Primary DC based on the project requirements.)

ii. Nature of replication between the DC and DRC (e.g., asynchronous or synchronous replication of data between Primary DC and DRDC)

RPO and RTO requirements (e.g., 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.). ***The RTO and RPO requirements are indicative only and the Government Department/Agency may modify based on the project requirements.***

iii. 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. In the event of a site failover or switchover, the

resources at the DR need to be scaled up to the required capacity at the DR of the application available at the Primary Data Center.

iv. 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 database storage should be 100% of the capacity of the Primary Data Center site.

v. 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 scaled up to the required compute capacity of the application available at the DC. The installed application instance and the database shall be usable. The use of this 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 the application should be routed seamlessly from DC site to DR site.

II. Platform as a Service (PaaS) Requirements

a. The PaaS Offerings shall support for the development, deployment and operation of custom applications.

b. PaaS shall provide a broad range of application infrastructure ("middleware") that supports a range of capabilities such as database management (with both SQL and NoSQL database), integration services, business process management, business analytics services, rules engines, event processing services and mobile back-end services.

c. PaaS offerings shall provide developers and operators with a "push and run" mechanism for deploying and running applications

d. The PaaS shall enforce separate environments based on application stage (dev/test vs. production). To ensure compliance and security, the platform has deployment policies based on lifecycle stage

e. The PaaS offerings shall support a range of runtime environments [Government Department / Agency may indicate the runtime environments required]

f. Configuration requirements shall be are kept to a minimum by default, at the same time offering the capability to control the configuration if required

g. The platform should include a database of the full application ecosystem (including what software is running on each host, who owns the application, and which versions are being used). This information should be available for the platform or for individual platform tenants.

h. Shall provide API Management capabilities - for ex: providing a level of control, so that only authorized users can access the API and each user can only access those capabilities for which they have permission.

i. PaaS offerings shall assist the application lifecycle by providing development tools including code editors, code repositories, build tools, deployment tools, test tools and services and security tools. The tools shall also include a set of application monitoring and analytics services, including capabilities such as logging, log analysis and app usage analytics and dashboards.

j. PaaS offerings shall provide dashboards and APIs that enable customers to plug in their own operations toolsets. So, for example, capabilities to increase or decrease the number of running instances of an application to deal with varying application load.

k. PaaS offerings shall provide built-in Security Capabilities or meet the security requirements as indicated by MeitY in the empanelment RFP reducing the load on developers and operators to provide these capabilities that include firewall, , secure protocol handling, access and authorization, encryption of data in motion and at rest, integrity checking, etc. PaaS systems shall offer these capabilities with minimal or no impact on application code, simplifying the programmer's tasks.

l. PaaS shall provide support for porting the existing applications so that the ported application will function correctly without the need for making modifications to the application

III. Virtual Desktop as a Service (VDaaS) Requirements

a. The service shall be available online, on-demand, and dynamically scalable up or down per request for service from the end users (Government Department/Agency or Government Department's nominated agencies) with two factor authentication via the SSL through a web browser.

b. The CSP providing VDaaS shall take full responsibility for hosting and maintaining the compute, storage, and access infrastructure, as well as applications and application

software licenses needed to provide the desktop service to the Government Department / Agency.

c. The CSP shall provide storage tiering, disk de-duplication, dynamic distribution of resources (bandwidth, CPU, and disk use), and flexible storage options supporting virtual machines.

d. The CSP shall provide secure application delivery in line with the security requirements mentioned in the RFP.

IV. DevOps as a Service (DevOps) Requirements

a. Provide tools to facilitate continuous deployment to production deployments through continuous delivery / integration practices and tools and provides the necessary functionality that when a deployment fails, it can be automatically rolled back to previous version. Developers should have the option and define the instances to which the application maybe deployed to

b. Provide a highly scalable, managed source control service that eliminates the need for Developers to operate your own source control system or worry about scaling its infrastructure.

c. Support “rolling deployments” so that a defined number of instances are available as configuration changes are made so that some instances are running to serve requests as other instances are being updated

d. Support Blue-green Deployments through DNS switching. This allows developers to switch domain name services (DNS) to make application deployments so that a new environment that has passed all the necessary tests and is ready to go live, can have traffic redirected to it and become the de-factor production environment while the old live environment now becomes the test bed for future deployments and vice-versa

e. DevOps tools must have a centralized log. The log shall maintain where apps were placed. This log must also be able to provide management and monitoring tasks to deployed application elements.

f. Allow the creation of scaling policies to act upon monitoring alarms that are triggered when defined thresholds are broken. Such a policy can result in an increase or decrease in the number of instances, depending upon the situation

Annexure 3 – Commercial Bid Formats

Annexure 3A - Commercial Bid - Pricing Summary Sheet

S. No.	Description	Total cost of excluding taxes and all other duties (1)	Total Applicable Taxes and all other duties (2)	Total Amount (INR) (3) = (1) + (2)	Total Amount in Words (INR) (3)
A	**Migration Services**				
B	**Operations and Maintenance / Managed Services Cost for a period of 2 [1] Years**				
C	**Operations and Maintenance – Managed Services Cost for the extended optional 1 Year**				
D	**Cloud Services – Setup Costs (if any)**				
E	**Cloud Services – Cost for pre-production and production Environment for 3 years – Requirements (On-Demand Pricing)** ***Provide Breakup as per Annexure 3B*** *(This is only for price discovery of cloud services and used for commercial evaluation. The actual payment will be on a pay-as-you-go model)*				

F	**Cost for pre-production and production Environment for 3 years – minimum commitment[2]** **Provide Breakup as per Annexure 3C** *(required only if the department is providing the minimum capacity required)*				
G	**Cost for Disaster Recovery / Business Continuity Services for 3 years for meeting the RPO / RTO requirements minimum commitment[2] (as per the format Annexure 3C)** *(required only if the department is providing the minimum capacity required)*				
H	**Cost[3] towards Support from the CSP**				
I	**Total Cost for Commercial Evaluation** **I = A + B + C + D + E+F+G**				

Note:

1. *The prices of cloud services could decrease therefore the contract duration are indicated for only two years (with an option to extend for an additional one year) to prevent vendor lock-in. However departments may consider the contact duration based on the project requirements.*
2. *This is required if department is indicating the minimum commitment of the resource requirements.*
3. *Include this line item if projects require support from CSP.*

Annexure 3B - Commercial Bid - Breakup of Cloud Services – Indicative/On-Demand pricing

This is to discover unit prices so that the department can pay on a pay-as-you go during the consumption of cloud services.

The Price Quote will be valid throughout the Contract Duration. This quote is only for commercial evaluation. The actual payment will be as per the usage and as defined in the payment terms section.

. No.	Description	Unit of Measurement for Pricing [To be filled by the department]	Unit Price (excluding taxes and all other duties) [To be filled by the bidder]	Multiplication Factor[1]	Total Price (excluding taxes and all other duties)	Total Applicable Taxes and all other duties	Total Price for Evaluation (Including taxes and all other duties)
		(1)	(2)	(3)	(4) = (2)* (3)	(5)	(6) = (4) + (5)
	Virtual Machines (*In case of requirement of VMs of different configuration, include individual line items providing the VM configuration (type of VM, number of virtual CPUs / cores, Speed, memory, storage,)*						
1.	Example: 2*4*20	Per Hour	To be Filled by the Bidder	Example: 1000 hours Or 3*365 x 24 hours [Years*days*hours]			
2.	……						
	Storage - *In case of requirement of Storage of different configuration, include individual line items providing the Storage configuration details*						
	Example : 512	per GB per Month	To be Filled by the Bidder	Example: 512/month for 12 months -512*12*3			
3.	…..						

. No.	Description	Unit of Measurement for Pricing [To be filled by the department]	Unit Price (excluding taxes and all other duties) [To be filled by the bidder]	Multiplication Factor[1]	Total Price (excluding taxes and all other duties)	Total Applicable Taxes and all other duties	Total Price for Evaluation (Including taxes and all other duties)
		(1)	(2)	(3)	(4) = (2)* (3)	(5)	(6) = (4) + (5)
4.	**Throughput**	per GB per Month	To be Filled by the Bidder				
	Other Cloud Services (e.g., ELB, PaaS…). ***Include individual line items as required for each of the Cloud Services***						
5.	**ELB**	Put an appropriate unit on which price is calculated		Put an appropriate multiplication factor that makes the figure significant for price comparison			
6.	**…..**						
	Additional Services - ***Include individual line items as required for each of the Services that are required to be implemented to meet the RFP requirements and that have commercial implications***						
7.	**Load Balancing**	Put an appropriate unit on which price is calculated		Put an appropriate multiplication factor that makes the figure significant for price comparison			
8.	**VLANs**	Put an appropriate unit on which price is calculated		Put an appropriate multiplication factor that makes the figure significant for price comparison			

. No.	Description	Unit of Measurement for Pricing [To be filled by the department]	Unit Price (excluding taxes and all other duties) [To be filled by the bidder]	Multiplication Factor[1]	Total Price (excluding taxes and all other duties)	Total Applicable Taxes and all other duties	Total Price for Evaluation (Including taxes and all other duties)
		(1)	(2)	(3)	(4) = (2)* (3)	(5)	(6) = (4) + (5)
9.	**…..**						
10.	**Any other tools required**						
11.	**Cost of retention of data beyond 45 days (shall include compute, memory… if required)** *(Departments may indicate the number of days based on the project requirements)*						

Note:

1. The Multiplication factor is used to arrive at a cost that would be a significant component in the commercial evaluation along with other costs such as Migration, O&M etc.

Annexure 3C - Commercial Bid - Breakup of Cloud Services (Minimum/Committed Quantity for 24 *365*2 Hours)

. No.	Description	Unit of Measurement for Pricing *[To be filled by the department]*	Unit Price (excluding taxes and all other duties) *[To be filled by the bidder]*	Quantity[1]	Multiplication Factor	Total Price (excluding taxes and all other duties)	Total Applicable Taxes and all other duties	Total Price for Evaluation (Including taxes and all other duties)
		(1)	(2)	(3)	(4)	(5) = (2)* (4)	(6)	(7) = (5) + (6)
	Virtual Machines - ***In case of requirement of VMs of different configuration, include individual line items providing the VM configuration (type of VM, number of virtual CPUs / cores, Speed, memory, storage,)***							
1.	Example: 2*4*20	Per Hour	To be Filled by the Bidder	Example: 4	Example: 4*24*365*3 hours [quantity*hours in a day*days in a year*no. of years] Or (Indicate total no. of hours)			
2.	**……**							
	Storage - ***In case of requirement of Storage of different configuration, include individual line items providing the Storage configuration details***							
3.	*Example : 512*	per GB per Month	To be Filled by the Bidder	Example: 2	Example: 512*2*12*3 [GB*quantity* months*years] Or (Indicate total GB required)			

. No.	Description	Unit of Measurement for Pricing *[To be filled by the department]*	Unit Price (excluding taxes and all other duties) *[To be filled by the bidder]*	Quantity[1]	Multiplication Factor	Total Price (excluding taxes and all other duties)	Total Applicable Taxes and all other duties	Total Price for Evaluation (Including taxes and all other duties)
		(1)	(2)	(3)	(4)	(5) = (2)* (4)	(6)	(7) = (5) + (6)
4.	**…..**							
5.	**Throughput**	per GB per Month	To be Filled by the Bidder					
	Other Cloud Services (e.g., ELB, PaaS …) ***Include individual line items as required for each of the Cloud Services***							
6.	**ELB**	Put an appropriate unit on which price is calculated			Put an appropriate multiplication factor that makes the figure significant for price comparison			
7.	**…..**							
	Additional Services - ***Include individual line items as required for each of the Services that are required to be implemented to meet the RFP requirements and that have commercial implications***							
8.	**Load Balancing**	Put an appropriate unit on which price is calculated			Put an appropriate multiplication factor that makes the figure significant for price comparison			
9.	**VLANs**	Put an appropriate unit on which price is calculated			Put an appropriate multiplication factor that makes the figure significant for price comparison			

. No.	Description	Unit of Measurement for Pricing *[To be filled by the department]*	Unit Price (excluding taxes and all other duties) *[To be filled by the bidder]*	Quantity[1]	Multiplication Factor	Total Price (excluding taxes and all other duties)	Total Applicable Taxes and all other duties	Total Price for Evaluation (Including taxes and all other duties)
		(1)	(2)	(3)	(4)	(5) = (2)* (4)	(6)	(7) = (5) + (6)
10.	**…..**							
11.	**Any other tools required**							
12.	**Cost of retention of data beyond 45 days (shall include compute, memory… if required)** *(Departments may indicate the number of days based on the project requirements)*							

Note:

1. The number of quantities may be indicated to the relevant line items.