Guidelines for Procurement of Cloud Services

Version 1.0

Ministry of Electronics & Information Tech., Government of India

Table of Contents

Table of Figures

1. Purpose

This document is prepared to provide guidelines to the Government Departments for procuring Cloud Services from the Cloud Service Provider (CSP), Managed Service Provider (MSP) and Systems Integrator (SI). The document will also highlight the key responsibilities of the Government Departments and the empaneled Cloud CSPs, MSPs and SIs during the Procurement of Cloud Services.

2. Background

MeitY announced the MeghRaj Policy to provide strategic direction for adoption of cloud services by the Government. 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.

For realizing the vision of MeghRaj policy, the Government Department will have to assess their requirement and procure Cloud Services from the CSP, MSP and SI accordingly. In order to do the same and realize full benefits of cloud adoption model, it is important for the Departments to understand their responsibilities in the entire adoption/migration process and what considerations should they keep in mind while drafting the Procurement RFP.

Below sections will explain in detail the responsibility of each of the stakeholders – Government Department, CSP, MSP and SI.

2.1 Empanelment of Cloud Service Offerings

Ministry of Electronics & Information Technology (MeitY) has empaneled multiple CSPs for three different Cloud Deployment Models:

1. Public Cloud
2. Virtual Private Cloud
3. Government Community Cloud

The CSPs empanel their cloud services offerings through GeM. The empaneled cloud services will be published through a GI Cloud Services Directory for use by government departments or agencies at the Centre and States.

Following are the Cloud service offerings offered by the CSPs for a combination of the Deployment Models:

1. Infrastructure as a Service (IaaS)
2. Platform as a Service (PaaS)
3. Software as a Service (SaaS)

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.

3. Procurement in Conventional IT Projects vs Cloud Service Projects

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 procurement of traditional on premise infrastructure and procurement of cloud computing.

Therefore, Departments need to be aware of the key considerations which need to be addressed when procuring cloud services. The key differences in procurement process are highlighted in the table below:

S. No.	Parameters	Procurement Process in Conventional IT Projects	Procurement Process in Cloud Computing 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	The Department may or may not undertake the estimation of the IT infrastructure resources for the entire project duration. The Minimum / Indicative** day one requirements can be indicated during the procurement process
2.	Flexibility to procure variable quantity of the same service	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.	Procurement scenarios	Since the requirements for the entire duration of project need to be specified in the RFP, the procurement becomes a Fixed Price procurement model	For cloud procurement, there are two scenarios 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

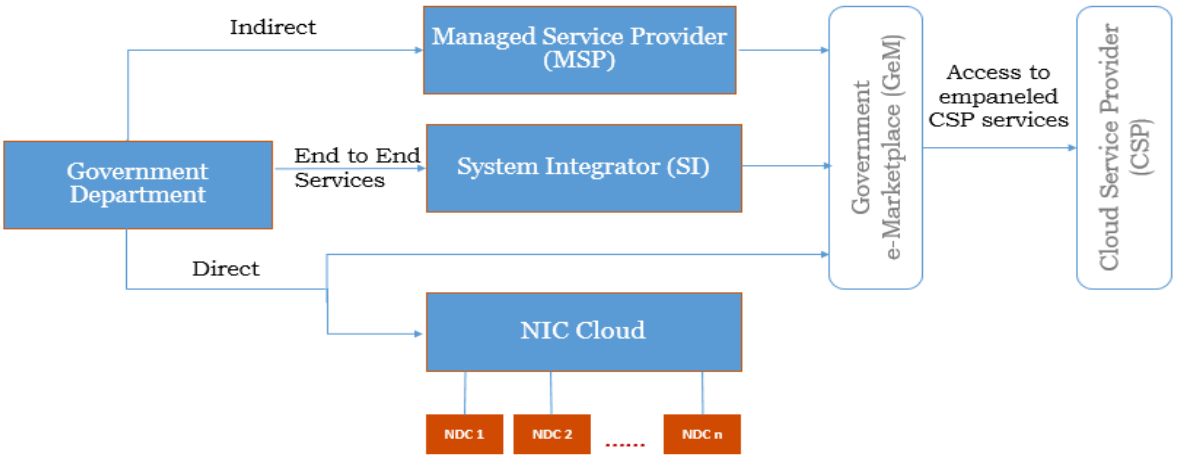
5.	Shared Responsibility	The responsibility of the project and deliverables lies with selected bidder	The responsibility of the Project, (owing to critical Security concerns) is shared between the CSP and the Department
6.	Standardized SLA	The conventional IT projects have largely well-defined and accepted SLAs across the project domains	SLAs critical to cloud services need to be identified and to be incorporated in the contract
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.
8.	Procurement cycle	Long procurement cycle	Quick procurement cycle
9.	Maintenance and upgradation	Traditional IT infrastructure devices (hardware and software) require maintenance and upgradation by the department itself	The focus is majorly on usage rather than maintenance. The CSP takes care of the underlying IT infrastructure used to provide Cloud Services. The Department/MSP is responsible for running and maintaining the applications on the Cloud platform.

****Indicative Requirements**: The Government Department can choose this model if the workloads are unpredictable. This model may result in high costs as an on-demand pricing is offered.

Minimum Requirements: The Government Department can estimate/predict the minimum workloads. As some minimum quantity is assured or committed by the Department, some CSPs/MSPs offer a discounted price.

4. Engagement models for procurement of Cloud Services

There are multiple scenarios or engagement models on how Government Departments can procure Cloud Services as indicated below. The Government Department/ Agency may choose the right scenario and accordingly specify the requirements in the RFP.



The Government Department can procure the Cloud Services in 3 different engagement models:

1. Procure Cloud Services directly from CSP
2. Procure Cloud Services through a MSP
3. Procurement of end to end services from a Systems Integrator

Each of the engagement models in explained below. This section of the document shall help in providing clarity, alignment & expectations of each stakeholder. The delineation of roles and responsibilities between all the stakeholders shall enable effective communication between the various stakeholders, facilitating adoption of Cloud in a smooth approach, increased internal control to the User Departments, improved process management and enhanced operational performance

4.1 Direct Procurement of Cloud Services from CSP

- **WHEN:**
  - Government Department / Agency will procure cloud services directly from CSP when it already has in place an Implementing Agency/Internal IT Team/expertise that is responsible for managing Cloud resources
  - In this scenario, the Government Department / Agency may consider migrating the existing application suite to Cloud and preparing an RFP to procure cloud service offerings OR
  - Government Department / Agency have a suite of legacy applications and /or plans to implement new solutions
- The department could also procure cloud services from re-sellers
- **Responsibility of Government Departments:** Government Department should have in place an Implementing Agency/Internal IT Team or expertise that is responsible for managing Cloud resources
- **Responsibilities of CSP:**
  - Offer services in accordance with the Cloud Service Model opted by the User Department
  - Offer the User Department with the elements such as facilities, data centers, network interfaces, processing, hypervisors, storage, and other fundamental computing resources where the department is able to deploy and run Cloud Service Model.
  - CSP shall be responsible for managing and controlling the underlying Cloud infrastructure including operating systems, storage, network, security, etc.

- Ensure successful network connectivity is established between the User Department location(s) and Cloud DC-DR site
- Ensure the appropriate security controls for physical and logical security are in place at Cloud DC and DR
- Ensure data is successfully replicated between the Cloud DC and Cloud DR and as per the required RPO specified by the User Department
- Ensure successful replication link is established between Cloud DC and DR site

4.2 Indirect Procurement of Cloud Services from MSP

- **WHEN:**
  - Government Department / Agency will procure cloud services from MSP when it does not have an Implementing Agency/Internal IT Team/expertise that is responsible for managing Cloud resource. In this case, they procure the Cloud services from MSP who will be responsible for managing the Cloud service offerings.
  - In this scenario, the Government Department / Agency have a suite of legacy applications and /or plans to implement new solutions OR
  - The Government Department / Agency have already identified an application
- **Responsibility of Government Departments:** The application responsibilities will remain with the respective Application Development Agencies. The Government Department will be responsible for implementation and operations of the application suite.
- **Responsibilities of MSP:**
  - MSP will be responsible for migrating to cloud and managing the cloud service offerings.
  - It is the responsibility of the MSP to monitor the cloud services (Resource Management, User Administration, Performance, Service Levels…).
  - Establishing connectivity between User Department's premise to Cloud DC and DR site
  - Deploying new applications on Cloud, user administration, security administration, planning and implementation of Cloud Management and Monitoring Portal for complete infrastructure and services procured
  - Monitoring & Reporting services
  - Exit management and billing management
  - Compute Services: Provisioning, installation, Configuration, Commissioning/De-commissioning and Management of the Virtual Machines and provide User Department the access to the same via secured web browser / Command Line Interface
  - Storage Services: Provisioning of scalable storage capacity as per requirements of the User Department and availability of services
  - Managed Database Services: Setting up, installation, configuration, management, upgradation and migration of Database Servers
  - Network Services: Maintain and manage the required networks components for the Cloud Services procured by the User Department
  - Security Services: Provisioning, Installation, Configuration, Management, Monitoring of Security Services as per the requirements of User Departments
  - Disaster Recovery Plan and Implementation: Setup and configuration of VMs, Storage, Network, Database, etc. at DR site meeting RPO and RTO requirements of the User Department

- Monitoring and Reporting Services: Deploy agent based monitoring for Cloud infrastructure monitoring and track system usage and usage reports

4.3 End to End Procurement of Cloud Services from a System Integrator

- **WHEN:** Government Department / Agency will procure end-to-end services from an SI when the cloud services would be a part of the total services procured through an SI for a turnkey project implementation.
- **Responsibility of Government Departments:** 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. : In this case, the The Government Department / Agency will enter in to a contract with each of them separately.
- **Responsibilities of SI:**
  - SI will perform all the responsibilities of the MSP (as mentioned above), along with the management of application suite
  - The underlying project infrastructure is provided by SI
  - SI will be responsible for the Application SLAs and the MSP will be responsible for the Cloud SLAs
  - Develop application / software to meet department needs / requirements
  - Manage application developed and host on Cloud
  - Hosting application on Cloud
  - Consult with User Department to understand business requirements
  - Conducting functionality tests
  - Conduct capacity sizing and planning for native applications

5. Key considerations during procurement of Cloud Services

Cloud services have been made available on the Government e-Marketplace (GeM) platform under the Professional Services -->> IT Services category. The Cloud services available on the GeM platform include the *Cloud Service Packages* which were initially made available in 2018 and the recent *individual Cloud services based on the Cloud Services Bouquet* prepared by MeitY.

Government organizations can procure Cloud services either through the GeM Marketplace or through the Bid Process / Reverse Auction (RA) functionality available on the GeM platform based on the total procurement value of the Cloud services.

The User Departments can refer to “Cloud Procurement Guidelines” for more details and assistance on how to procure Cloud services through GeM.

Procurement of Cloud Services is a lengthy process and involves multiple phases with critical roles and responsibilities of all the stakeholders in each phase. It is important that the right people do the right things at the right time.

Ideally, there are five phases involved when the Government Department plans to procure Cloud services or migrate to Cloud:

1. Planning
2. Design
3. Procurement and Implementation
4. Operations and Maintenance
5. Exit Management/Transition Out

Each phase is goal oriented and ends at a particular milestone. The following sections will explain the key responsibilities of the Government Department and the CSP, MSP and SIs in detail.

If any User Department decides to procure Cloud Services directly through a CSP and does not onboard a MSP or a SI, the responsibilities of MSP /SI as defined above and below in this document shall be applicable to the User Department.

5.1 Planning Phase

The Government Department needs to draft a proper plan for procurement of Cloud Services. This planning will help the Department to manage the subsequent phases effectively. The Planning phase is essentially driven by the Government Department. The Department can take the help of MSP/SI/external agency while planning and designing phase. This scope needs to be clearly mentioned in the RFP.

Parameter	User Department Responsibility	CSP Responsibility	MSP/SI Responsibility
Service Model Requirements	• Based on the project requirements, the Government Department may choose to procure one/some of the Service Models empaneled by MeitY (IaaS, PaaS, SaaS) and indicate any additional requirements over and above the requirements mentioned in the Empanelment Compliance Requirements. • For more details on the Cloud service models, please refer to Annexure 2		
Indicative Requirement vs Minimum Requirement	• The Government Departments need to estimate the requirements of infrastructure resources (like Virtual Machines, Storage etc.) based on the application, workload etc. for different environments such as Production and Non Production. • 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. • The Department must make sure that their technical requirement and budget estimation is done keeping in mind the future requirement, minimum 3 years ahead. • Additionally, the indicative requirements or the minimum assured requirements need to be mentioned to obtain quotes from the MSPs. • For more details on Indicative and Minimum requirements, please refer to Annexure 3		

5.2 Design Phase

This is an early phase of a project where the key Cloud requirements and services are planned out. The Government department shall transform the requirements into a complete and detailed technical specifications. In this phase, the Government Department will provide sufficient information to the MSPs so that they can customize their solution and share their best solution and costing.

Parameter	User Department Responsibility	CSP Responsibility	MSP /SI Responsibility

Application Environment to be set up	• The Government Department/Agency shall indicate the requirement of the Production and Non Production environments based on the project requirements and will define the choice of the deployment model - public / virtual private / government community.
	• There are two types of data center environments and the selection between them is based upon the Government Department's project requirements:
	  ○ **Production Environment:** This is a type of DC environment where the software and applications are actually put into operation for their intended use by end users.
	  ○ **Non Production Environment:** This is a type of DC environment where the hardware, software, applications etc. are tested and debugged. This environment consist of various sub stages like pre-production, testing and staging environments. This is a purely non-live environment.
	• Departments may indicate a requirement for both the environments with the flexibility to scale up or scale down based on the requirements. The environments (public / virtual private / government community) shall comply with the respective Empanelment Compliance Requirements.		

Software Licenses	• **Department has an existing software license:** 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 MSP 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. • **Department needs to procure software license:** 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.		

Parameter	User Department Responsibility	CSP Responsibility	MSP /SI Responsibility
MSP Support Requirements	• MSP 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 MSP as a part of the RFP.		
Additional Requirements	• Though the responsibilities and mandatory compliances of the empaneled CSPs have already been ensured through the MeitY empanelment RFP, the User Department must re-check the validities and list down additional requirements, if any. • Government Department may specify some additional requirements for security, data backup, exit management price discovery etc. in the RFP. The guidelines for each of the requirement is mentioned in section: o **Additional Security Requirements** : Security features like PCI – DSS, Data Encryption, Third Party Authentication Support etc. as per the requirements of the data handled by the Government Department / Agency o **Auto Scaling Limit :** This is a service that automatically monitors and adjusts compute resources to maintain performance for applications o **Data Retrieval Period** : Length of time in which the Government Department can retrieve a copy of their cloud service customer data from the cloud service o **Data Retention Period** : Length of time for which the MSP will retain backup copies of the customer data during the termination/closure process. As per the Empanelment RFP, the CSP should not delete any data before 45 days from the expiry of the contract and the MSP will ensure the compliance of the same. o **Log Access Availability** : This parameter ensures the access of log file entries that the customer can access o **Logs retention period** : The period of time during which logs are available for analysis		

Parameter	User Department Responsibility	CSP Responsibility	MSP /SI Responsibility
	○ **Backup Requirements** : Departments should indicate the estimated size of data ○ **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 ○ **Data Backup Method** : List of method(s) used to backup cloud service customer data ○ **Data Backup Frequency** : The period of time between complete backups of data ○ **Backup Retention Time** : The period of time a given backup is available for use in data restoration. As per the Empanelment RFP, the CSP should provide a backup solution that supports retention period of minimum 30 days or as desired by the User Department as per their needs. ○ **Backup Generations** : The number of backup generations available for use in data restoration ○ **Maximum Data Restoration time** : The committed time taken to restore cloud service customer data from a backup ○ Provide support for automation tools for data portability ○ **Data portability format** : The electronic format(s) in which cloud service customer data can be transferred to/accessed from the cloud service ○ **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 ○ **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 ○ **Platform migration** : P series / SPARC to X86, OS migration requirements may be indicated if required for the project.		

Parameter	User Department Responsibility	CSP Responsibility	MSP /SI Responsibility
	• **Exit Management Cost :** The Departments must discover the MSP's exit prices, in terms of effort (man month, bandwidth, relevant tools etc.) during exit or the unit rate of transfer of data, application or VMs		

5.3 Procurement and Implementation Phase

Parameter	User Department Responsibility	CSP Responsibility	MSP/SI Responsibility
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.	• Provide self-service tools to the Government Departments that can be used to manage their Cloud infrastructure environments including Government Department specific configurations • Provide interoperability support with regards to available APIs, data portability etc.	• Study of existing user department setup (if applicable) • Establishing connectivity between User Department's premise to Cloud DC and DR site • Migration of existing applications / data to Cloud and vice versa • Deploying new applications on Cloud, user administration, security administration, planning and implementation of Cloud Management and Monitoring Portal for complete infrastructure and services procured • Setting up of DR site (if applicable) • Monitoring & Reporting services • Exit management and billing management

Procurement of Infrastructure Services	• 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. • Providing approvals to CSP/MSP/SI for all types of request(s) submitted	• Provision and offer services in accordance with the Cloud Deployment Model • Provide User Department with Data Centers and Network Interfaces • Provide Compute, Storage, hypervisors and other fundamental compute resources • Provide auto-scalable, redundant, dynamic computing capabilities or virtual machines • Ensure network port connectivity for links between the User Department location(s)/Infrastructure and other Cloud environments (DC/DR)	• The MSP manages the security of Facilities, Physical security of hardware , Network infrastructure and Virtualization infrastructure

Parameter	User Department Responsibility	CSP Responsibility	MSP/SI Responsibility
Procurement of Platform Services	• The department has 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	• The CSP manages the underlying infrastructure and foundation services, the operating system and the application platform. • The CSP platform may provide data	• Manage (including project managing), coordinating and planning all aspects of migration • Proactively identify, monitor and manage any significant risks or issues in relation to migration • Provide regular progress reports to the Government Department / Agency ○ A listing of all Migration Deliverables and Milestones, including acceptance status, the estimated time to

	may provide security groups and allow the department to manage firewall rules through the CSPs security groups for the instances. • Implement and configure the tools provided by CSP based on the project requirements. • Ensure that the CSP facilities/services are certified to be compliant to the standards as mentioned below • Providing approvals to CSP/MSP/SI for all types of request(s) submitted	backup and recovery tools • Security tools are provided by the CSP • The CSP shall be responsible for to provide infrastructure and platform service(s) (such as middleware) to run the applications created using programming languages, libraries, services, and\ tools supported by the CSP, on selection of PaaS Cloud Service Model by the User Department. • Provide auto-scalable, redundant, dynamic computing capabilities	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) ○ 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 • Status of the any risks, including those identified in the Risk Management Plan, as well as the steps being taken to mitigate such risks

Parameter	User Department Responsibility	CSP Responsibility	MSP/SI Responsibility
Procurement of Software Services	• User Department will be responsible for compliance with the Contract, Documentation and Order Forms • Government Department will be responsible for the accuracy, quality and legality of their data, the means by which the Department acquired this data and the use of data with the services	• CSP shall be responsible offer the User Department with applications running as a service, along with its security, network, storage requirements, upgradation of application, its maintenance and performance, on selection of SaaS, as a Cloud Service Model by the User Department. • To provide in-built functionality to integrate with existing authentication mechanisms like Active-Directory	• MSP will be responsible for managing the platforms and services provided by the third

		• To ensure that any service offered from SaaS are monitored, controlled and administered using web based tool with visibility to the User Department. • To ensure that services offered under SaaS are available with automatic scale up (adding more resources to handle demand) and scale out (adding more systems to handle demand) to meet User Department's performance requirements.	party vendors

Parameter	User Department Responsibility	CSP Responsibility	MSP/SI Responsibility
Security	• Configuring their IT environments in a secure and controlled manner for their security purposes • Review and validate security configurations created by CSP / MSP • Departments 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 27017** - Code of practice for information security controls based on ISO/IEC 27002 for	• To ensure all the compliances as defined by MeitY for empanelment of Cloud Services offered by CSP and the security guidelines as defined by STQC are met by the CSP • Providing services on a highly secure and controlled platform and providing a wide array of security features customers can use. • There are a lot of Security tools offered by the CSP, like: ○ Identity and Access Management (IAM) ○ Multi-Factor Authentication (MFA) ○ Encryption of data associated with VM ○ DDoS Protection (safeguards web applications running on cloud) ○ TSL/SSL Certificate Management	• MSP will control and manage the tools provided by the CSP. • Provisioning, Installation, Configuration, Management, Monitoring of Security Services as per the requirements of User Departments. • Maintain and manage access control with Network Security Groups, NACL and routing tables • Identifying Security Configuration gaps • Provision, manage and deploy HSM (High Security Module) as per User Department(s) requirement • Implementation of tools such as; IPS, IDS, SIEM • Conduct Security / Risk Assessment • Implementation of Multi-Factor Authentication Services • Comprehensive Application security

	cloud services and Information technology ○ **ISO 27018** - Code of practice for protection of personally identifiable information (PII) in public clouds. ○ **ISO 20000-1** – NOC and SOC facility must be within India for the Cloud Environments and the managed services quality should be certified for ISO 20000:1 ○ In addition to the certifications mentioned in the Empanelment RFP, the User Department may also seek for PCI DSS certified CSPs (based on their requirement). This is a compliant technology infrastructure for storing, processing, and transmitting credit card information in the cloud		• Implementation, management and monitoring of DDoS, IPS, IDS technology and solutions to ensure the security of Cloud Services procured • Installation, Configuration, Implementation and management of Log Analyzer • 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 • Deploy security patches on hardware and software • Take regular backups of security configurations

Parameter	User Department Responsibility	CSP Responsibility	MSP/SI Responsibility
Migration	• Decide on Data / Applications to be migrated	• Provide relevant tools and services for backup, migration and replication of applications / data	• 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: ○ **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: ✓ 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 ✓ Procedures and documentation to be developed for migration of applications and data & content including redevelopment/additional development that may be required ✓ Plans for co-existence of non-cloud and cloud architectures during and after migration ✓ Communication, change management, and training needs ✓ Cloud governance for post-implementation ✓ Test Plans for verifying successful migration ✓ Detailed Risk Management Plan that will identify potential risks, set out possible mitigation approaches, and identifies specific tasks the MSP will undertake to help avoid identified risks connected with the Migration. ○ **Migration Process:** ✓ 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 ✓ Analysis of the interdependencies such as application dependencies and affinities to servers, server configuration etc. ✓ Dependencies between applications and data

			✓ 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 ✓ 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. ✓ Configuring external connections to the hosted infrastructure required to upload database backups and virtual machine (VM) images to the hosting environment. ✓ 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. ✓ To enable easy migration to cloud, Department may consider up-gradation of OS & DB to latest version available in market. ✓ Deployment of the new Applications on the cloud environment as per the TO BE Architecture. ✓ Configure, manage, deploy, and scale the system on environments setup on cloud

5.4 Operations 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 CSP/MSP.

Parameter	User Department Responsibility	CSP Responsibility	MSP/SI Responsibility
O&M	• Department monitors the operational activities to ascertain that the MSP/SI has implemented the cloud features mentioned in the RFP.	• 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	• 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,

	• 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 features to enable departments to monitor the performance, security, resource utilization etc.	service operates will be the responsibility of the CSP • Manages IT controls associated with the physical infrastructure deployed in the cloud environment	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. • Interface with the CSP(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. • Prepare a comprehensive O&M plan for managing the cloud services and keep it updated with any changes during the course of the project. • Create and maintain all the necessary technical documentation, design • documents, standard operating procedures, configurations required to continued operations and maintenance of cloud services.

Parameter	User Department Responsibility	CSP Responsibility	MSP/SI Responsibility
Resource Management			• 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. • 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 MSP, based on the growth in the user load (peak and non-peak periods; year-on-year increase),

			will manage the scale up or scale down of compute, memory, storage, and bandwidth to support the scalability and performance requirements of the solution and meet the SLAs. • 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. • 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 MSP 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. • 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. CSP 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. • Provisioning and configuring their implementation of storage and virtual machines that allows for the MSP to launch and terminate cloud instances, change firewall parameters, and perform other management functions. Upon deployment of virtual machines, the MSP has to assume full administrator access and is responsible for performing additional configuration, patching, security hardening, vulnerability scanning, and application installation, as necessary. • For the underlying system software (procured under platform as a service), the CSP shall provide the Annual Technical Support (ATS) from the OEM during the entire period of the contract.

User Administration	• The Government Department will share the list of users that can access the Cloud applications and the privileges that each of them will carry • Specifying the roles of users for managing access to data / application		• 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) • 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. • Implement multi-factor authentication (MFA) for the root account, as well as any privileged Identity and Access Management accounts associated with it.
Security Administration and monitoring Security Incidents	• Ensuring the security of the endpoints that are used to access Cloud services (as applicable)		• Appropriately configure the security groups in accordance with the Government Department / Agency's networking policies • Regularly review the security group configuration and instance assignment in order to maintain a secure baseline. • Secure and appropriately segregate / isolate data traffic/application by functionality using DMZs, subnets etc. • Ensure that the cloud infrastructure and all systems hosted on it, respectively, are properly monitored for unauthorized activity. • 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. • Conducting regular vulnerability scanning and penetration testing of the systems, as mandated by their Government Department / Agency's policies. • Review the audit logs to identify any unauthorized access to the government agency's systems.

Monitoring Performance and Service Levels (Availability, Incident Management, Performance)			• 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. • Reviewing the service level reports, monitoring the service levels and identifying any deviations from the agreed service levels • 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 • Receiving and processing service level reports from the CSP (or a trusted third party (auditor), comparing them with SLA objectives. • Detecting and reporting service level agreement infringements • Responding to SLA infringements either as reports from the CSP or detected by MSP or Government Department / Agency (for example, informing their end-users of service interruptions, raising a ticket, claiming service credits etc.) • Resolving disputes around SLA infringements • Provide and document patch management appropriate to all components within the CSP's boundary and to adhere to Government Department/Agency or MietY standards, if any. • 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 CSP's boundary.
Backup	• Formulate a Backup Policy	• Provide relevant tools and services for backup, migration and replication of applications / data	• Files & Images: Frequency for full backups and incremental backups • Databases and log files: Frequency for full backups and incremental backups • Off-site backup requirement that still meets the prescribed RTO requirements> • 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 • Files & Images: Retention timelines of inactive versions of the backups

			• Databases & log files: Retention timelines of inactive versions of the backups • Preservation and Retention of Data [required for certain domain specific projects] • 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. • Administration, tuning, optimization, planning, maintenance, and operations management for backup and restore; • Provision capacity for backup and restore, as required • Perform backup on the next scheduled backup window in case of any scheduling conflicts between backup and patch management.
Usage Reporting and Billing Management	• Department / Agency to validate the billing and SLA related penalties		• Track system usage and usage reports • Monitoring, managing and administering the monetary terms of SLAs and other billing related aspects. • Provide the relevant reports including real time as well as past data/information/reports for the Government • Track system usage and usage reports • Provide relevant reports including real time as well as past data/information/reports for user Departments • Summary of resolved, unresolved and escalated issues / complaints • Logs of backup and restoration undertaken report • Component wise Virtual machines availability and resource utilization report • Consolidated SLA / Non- conformance report • Any other activity associated with Reporting Services • CRUD Operations: MSP to Create, Read, Update, Delete, users based on roles & rights defined by User Department • Prepare Monitoring Reports • Prepare SLA Reports • Prepare Backup Reports • Prepare VMs Status report • Provisioning /De-provisioning of VMs • Creating templates for VMs • Make changes in configurations for user administration

			• Any other activity associated with operations and management of Cloud Management Portal
Disaster Recovery	• Departments need to mention the responsibilities of the MSP clearly in the RFP. • The Department need to ensure that they mention the exact and correct requirement for disaster recovery	• Offer DR Services meeting DR requirements of the User Department	• 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. • Sizing and providing the DC-DR replication link so as to meet the RTO and the RPO requirements. • 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 DR or vice-versa (regular planned changes), there should not be any data loss and should meet the RTO and RPO requirements. The MSP shall clearly define the procedure for announcing DR based on the proposed DR solution. The MSP shall also clearly specify the situations in which disaster shall be announced along with the implications of disaster and the time frame required for migrating to DR. The MSP shall plan all the activities to be carried out during the Disaster Trial and issue a notice to the Government Department/Agency at least two weeks before such trial. • Setup and configuration of VMs, Storage, Network, Database, etc. at DR site meeting RPO and RTO requirements of the User Department • Replication tool and mechanism between DC and DR site • Network connectivity from User Department to DR site • DR drills should could be conducted once every six months • Define the procedure for announcing DR based on the proposed DR solution. • 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.

			• Plan the activities to be carried out during the Disaster Drill and issue a notice to the Department at least 15 working days before such drill. • RPO monitoring, reporting and event analytics for the disaster recovery solutions • Automated switchover/ failover facilities (during DC failure & DR Drills). • Any other activity associated with operations and management of DR Plan and Implementation
Support Third Party Audit and other requirements		• Provide support during Audit by STQC / Meity empaneled agency or any agency appointed by the User Department.	• 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.

Parameter	User Department Responsibility	CSP Responsibility	MSP/SI Responsibility
Monitoring Tools	• The departments may ensure that the MSP/SI implements tools/services that provide the features 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.	• Provide relevant tools and services for monitoring the performance, security, resource utilization etc.	• Deploy agent based monitoring for Cloud infrastructure monitoring • Monitor 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 • Monitor Internet links, Replication links, MPLS, P2P (as applicable), including but not limited to Bandwidth utilization,

	○ 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.		Data transfer, Response time \(latency) and Packet loss. • Monitor Daily, weekly, monthly backup jobs as per schedule and during any unsuccessful backup the incident management process and procedures should be invoked. • To perform regular health checks of VMs, Storage, N/w links, etc. • Review the service level reports, monitoring the service levels and identifying any deviations from the agreed service levels • Implement necessary tools to monitor the root cause for performance degradation of any applications. User Department should be able to analyze whether issue is actually an Application issue or Hosting/hardware/Bandwidth issue. • Investigate outages; perform appropriate corrective action to restore the hardware, software, operating system, and related tools • Investigate outages; perform appropriate corrective action to restore the hardware, software • Any other activity associated with Monitoring Services
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. • 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.		

5.5 Exit Management/Transition Out Phase

The responsibilities of each stakeholder should be clearly delineated in the RFP, during the exit management period.

Parameter	User Department Responsibility	CSP Responsibility	MSP/SI Responsibility
Exit Management	• 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 MSP, CSP and the Systems Integration. • The departments can procure Disaster Recovery, Exit Management Services, Operations & Management Services, Migration and Provisioning Services, Back	• To provide support to the User Department for transferring data / applications at the time of exit management and as per the guidelines defined by MeitY in Cloud Services empanelment RFP.	• Assist the Department in migrating the VMs, data etc., and should ensure destruction of data • Migration of the VMs, data, content and any other assets to the new environment or on alternate CSP'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. • The format of the data transmitted from the CSP to the Department should leverage standard data formats (e.g., OVF, VHD…) whenever possible to ease and enhance portability. • 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.

	up and Support Third Party Audit and other requirements as a Managed Service.		• Ensure that all the documentation required for smooth transition including configuration documents are kept up to date • Ensure that the CSP does not delete any data at the end of the contract (for a minimum of 45 days beyond the expiry of the contract) 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. • 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. • Provide a comprehensive exit management plan. • 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 CSP's offerings to enable successful deployment and running of the Government Department's solution on the new infrastructure. • Address and rectify the problems with respect to migration of the Government Department / Agency application and related IT infrastructure during the transition. • Ensure that all the documentation required by the Government Department / Agency for smooth transition (in addition to the documentation provided by the CSP) 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. • 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. • 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 contract.

6. Payment Terms

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.

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

6.1 Payment milestones for the Cloud Services Consumed

S. No.	Phase	Milestone	Amount
1	Monthly Payments (The first monthly payment will be due on completion of one month 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

Payment for Cloud Services

1. Monthly/Quarterly 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 MSP after any SLA related deductions.

6.2 Payment milestones for the Managed Services consumed

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 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 OR **Initial setup cost**	On signing of contract and fulfillment of conditions precedent including submission of advance bank guarantee of equal amount	0 to 30% of the total project cost
		Initial cost is to be paid when the MSP gives a go live of the requested services	
2	Successful Completion of Migration/initial completion of setup/committed milestones	Successful Migration of existing system to Cloud environment and sign-off from the Government Department / Agency	70% to 100% of milestone cost after completion of that milestone

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

Payment for Managed Services:

1. EMI to be made at the end of the month/quarter after satisfactory delivery of the services
2. Total Monthly/Quarterly payment should be linked to the compliance with the SLA metrics and the actual payment due to the MSP after any SLA related deductions
3. Additional Services: Government Department / Agency have the option to avail the additional services of MSP 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 contract. The unit costs, where available, quoted in the commercial proposal will be used for such approved additional work.

6.3 Payments if SI is engaged to provide end to end services

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 4. 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.

7. Annexure 1: 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:

- 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
- 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, SaaS) 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.

8. Annexure 2: Service Model Requirements

- **Infrastructure as a Service (IaaS):** The CSP shall provide the compute, storage, networks, and other fundamental resources where the consumer is able to deploy and run arbitrary software. The CSP shall be responsible for managing and controlling the underlying Cloud infrastructure including operating systems, storage, network, security, etc. and the deployed applications shall be managed and controlled by the User Department.
- **Platform as a Service (PaaS):** The CSP shall provide the Cloud infrastructure and platform (such as middleware) to run the applications created using programming languages, libraries, services, and tools supported by the CSP. The User Department shall not manage or control the underlying Cloud infrastructure including network, security, servers, operating systems, or storage, but has control over the deployed applications and possible configuration settings for the application-hosting environment.
- **Software as a Service (SaaS):** The CSP shall offer its applications running on the Cloud infrastructure as services. The applications shall be accessible from various client devices through either a thin client interface, such as a web browser or through a programming interface. The User Department shall not manage or control the underlying Cloud infrastructure, platform and application landscape including network, security, servers, operating systems, storage, or even individual application capabilities with the possible exception of limited user-specific application configuration settings.

a. Specific Requirements for 'Infrastructure as a Service' (IaaS)

The below mandatory requirements are applicable in addition to common technical controls for services offered by CSP from service model 'Infrastructure as a Service', using Government Community Cloud or Virtual Private Cloud or Public Cloud as Cloud Deployment Models.

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

- The Service shall provide auto-scalable, redundant, dynamic computing capabilities or virtual machines.

- Service shall allow Government Department empaneled users to procure and provision computing services or virtual machine instances online with two-factor authentication via the SSL through a web browser.

- 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.

- 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 User Department(s) required format.

- 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.

- 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 is not forensically recovered.

- CSP shall ensure that VMs receive OS patching, health checking, Systematic Attack Detection and backup functions.

- Monitor VM up/down status and resource utilization such as RAM, CPU, Disk, IOPS and network.

- The respective Government Department shall retain 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.

- 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.

- CSPs shall manage CSP provisioned infrastructure including VMs as per the ITIL standards.

b. Specific Requirements for 'Platform as a Service' (PaaS)

The below mandatory requirements are applicable in addition to common technical controls for services offered by CSP from Platform as a Service, using Government Community Cloud or Virtual Private Cloud or Public Cloud as Cloud Deployment Models.

- CSPs shall be responsible for development, deployment, operations and support of custom applications or any application procured by the User Department from Platform as a Service.

- CSPs shall ensure multiple range of runtime environments are supported to enable User Departments to choose the most appropriate technology for the task.

- CSPs shall be able to control the number of parallel running instances of an application in order to handle the anticipated workload or to meet resiliency goals.

- CSPs shall ensure that any services offered from Platform as a Service are portable and vertically integrated.

- CSPs shall ensure that services offered from Platform as a Service are available with automatic scale up (adding more resources to handle demand) and scale out (adding more systems to handle demand) to meet User Department's performance requirements.

- CSPs shall ensure that any service offered from Platform as a Service have 99.50 % UPTIME and there is no compromise on performance of the application.

- CSPs shall be responsible to clearly demonstrate to MeitY / STQC or any 3rd party assessor appointed by STQC at the time of getting its services empaneled on how to get existing data into the solution and any new or updated data back again.

- CSPs shall ensure that User Departments are provided with Central web based tool for monitoring and management of services.

c. Specific Requirements for 'Software as a Service' (SaaS)

The below mandatory requirements are applicable in addition to common technical controls for services offered by CSP from Software as a Service, using Government Community Cloud or Virtual Private Cloud or Public Cloud as Cloud Deployment Models.

- Cloud services under SaaS model shall only be offered from Data Centers audited and qualified by STQC under the Cloud Services Empanelment process.

- CSPs shall be responsible for ensuring that all data functions and processing are performed within the boundaries of India.

- CSPs shall be responsible to ensure that the services offered from SaaS provide a mechanism to authenticate and authorize users.

- SaaS solution / services offered to User Departments shall have in-built functionality to integrate with existing authentication mechanisms like Active-Directory.

- SaaS solution shall be able to segregate users on basis of privileges granted to the users.

- CSPs shall provision and implement role-based authentication when required and separation of identities shall be maintained in multi-tenant environment.

- CSPs shall ensure that all the policies and procedures shall be established and maintained in support of data security to include confidentiality, integrity, and availability across various system interfaces and business functions to prevent any improper disclosure, alternation, or destruction.

- CSPs shall ensure that any service offered from SaaS are monitored, controlled and administered using web based tool with visibility to the User Department.

- CSPs shall ensure that User Departments are provided with capability to generate custom reports around several parameters such as users, time, data, etc.

- CSPs shall be responsible to provide a mechanism to enable each User Department's administrator to create, manage and delete user accounts for that tenant in the user account directory.

- CSPs shall ensure that services offered under SaaS are available with automatic scale up (adding more resources to handle demand) and scale out (adding more systems to handle demand) to meet User Department's performance requirements.

- CSPs shall ensure that any service offered from the SaaS solution provider comply with PII data security standards like ISO 27018.

- CSPs shall ensure that services offered under SaaS are enabled with data loss prevention tools and capability to monitor data flow.
- CSPs shall ensure that services offered under SaaS provide tools / capability for encryption of data-at-rest, data-in-processing and data-in-transit.
- CSPs shall ensure that services offered under SaaS support encryption algorithms like AES256 and higher

The below figure explains the control and responsibility of Government Departments/MSP and CSP for each of the Cloud Service model.

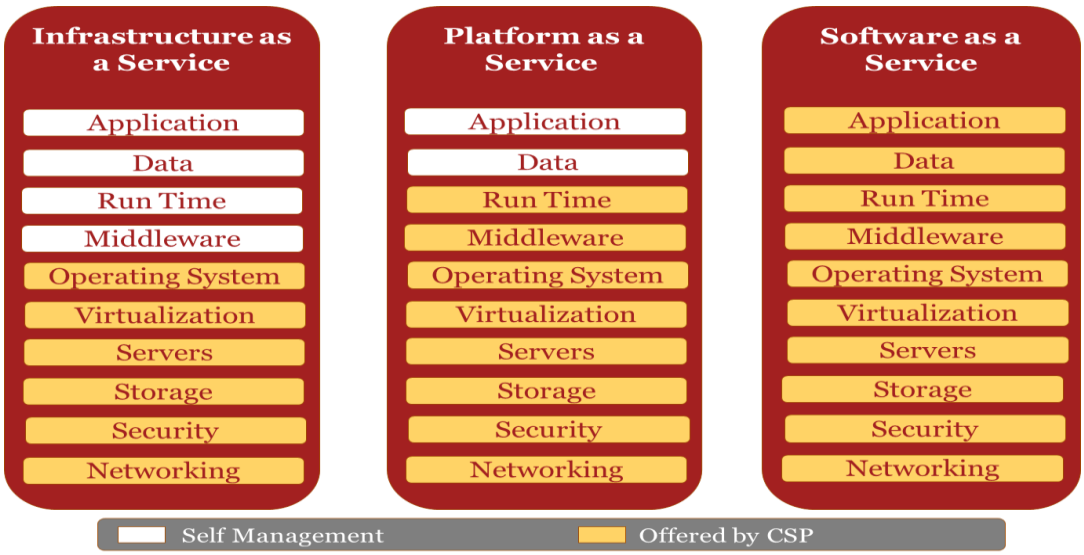


Figure 1: Cloud Service Models

9. Annexure 3: Indicative Requirement and Minimum Requirement

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 indicative day-one operating requirements or minimum assured requirements. The Department must make sure that their technical requirement and budget estimation is done keeping in mind the future requirement, minimum 3 years ahead.

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

Below is a an example of Indicative requirements. The Government Departments are free to choose their own configurations/description based on the requirement. The service configurations can be referred from Cloud Service Bouquet Document. In case the Government Department wants to mention 'Minimum requirements', they need to mention the quantity of each service in addition to the below information.

Example: 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	Indicative Projections		
				Year1	Year2	Year3
Virtual Machine Service						
1.	Example: **OS:** MS Windows Server **vCPU:** 4 **RAM:** 128GB **Storage:** 50GB HDD **CPU Launch Year:** Beyond year 2015 **Physical Core to vCPU Ratio:** 1:2	Hourly/Monthly/Yearly	Example: 1000 hours			
Storage Service						
2.	**Block Storage Example:** **Storage Type:** HDD **Storage Amount:**1000GB **IOPS:** 1001-2000	Hourly/Monthly/Yearly	Example: 1000 hours			

3.	**Object Storage Example:** **Storage Amount:** 1000GB	Hourly/Monthly/Yearly	Example: 1000 hours			
4.	**File Storage Example:** **Storage Amount:** 1000GB	Hourly/Monthly/Yearly	Example: 1000 hours			
5.	**Archival Storage Example:** **Storage Amount:** 1000GB	Hourly/Monthly/Yearly	Example: 1000 hours			
Database Service						
6.	**Managed Database as a Service Example:** **Database Service Name:** MS SQL Web Edition **vCPU:** 8 **RAM:** 128GB **Storage:** 50GB HDD **CPU Launch Year:** Beyond 2015 **Physical Core to vCPU Ratio:** 1:2	Hourly/Monthly/Yearly	Example: 1000 hours			
Network Service						
7.	**Virtual Network:** There is no Service Procurement Parameter for this service. All CSPs provide virtual network / subnet capability by default to their customers without any extra cost. However, resources used within the virtual network / subnet may be charged by the CSPs.	NA	NA			
8.	**Load Balancer Example:** **Service Name:** Network Load Balancer (Virtual/Physical) **Throughput:** 1000MBPS	Monthly/Yearly	Example: 12 months			
9.	**Firewall Example:** **Throughput:** 1000MBPS	Hourly/Monthly/Yearly	Example: 1000 hours			
10.	**Public IP Example:** **Type of IP:** Static **No. of IPs needed:** 8	Hourly/Monthly/Yearly	Example: 1000 hours			
11.	**Web Application Firewall Example:** **Throughput:** 1000MBPS	Hourly/Monthly/Yearly	Example: 1000 hours			

Security Service						
12.	**Active Directory Service** **Example:** **No. of users:** 301-400	Monthly/Yearly	Example: 12 months			
Support Service						
14.	**Enterprise Support Service** **Example:** (i) 24x7 access to email, chat and phone support to notify and register the incidents (ii) 24x7 support for general guidance (iii) Response to be made available within 15 minutes for Business Critical System outage	Monthly	Example: 12 months			

Note: 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 CSP shall continue to develop and refine infrastructure in accordance with emerging requirements and evolving technology specifications as required.

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.*

10. Annexure 4: Commercial Bid Formats

Annexure 4A - Commercial Bid - Pricing Summary Sheet

S. No.	Description	Total Cost excluding taxes & all duties (1)	Total applicable taxes and all duties (2)	Total Amount (INR) (3) = (1) + (2)	Total Amount in Word (INR) (3)
A	Migration services				
B	Operations and Maintenance / Managed Services Cost for a period of 2 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 4B (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.				

	Provide Breakup as per Annexure 4C (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 (as per the format Annexure 3C). (Required only if the department is providing the minimum capacity required)				
H	Cost towards Support from the CSP – (Include this line item if projects require support from CSP)				
I	Exit Management Cost (termination or closure)				
J	Total Cost for Commercial Evaluation I = A + B + C + D + E + F + G + I				

Annexure 4B - 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 usage and as defined in the payment terms section.

S. 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	Multiplication Factor[1]	Total Price (excluding taxes and all duties)	Total Applicable Taxes and all duties	Total Price for Evaluation (Including taxes and all 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						
3.	*Example : 512*	per GB per Month	To be Filled by the Bidder	Example: 512/month for 12 months -512*12*3			
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			
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 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 4C - Commercial Bid - Breakup of Cloud Services (Minimum/Committed Quantity for 24 *365*2 Hours

S. 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	Multiplication Factor[1]	Total Price (excluding taxes and all duties)	Total Applicable Taxes and all duties	Total Price for Evaluation (Including taxes and all 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)			
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			
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: The number of quantities may be indicated to the relevant line item