Guidelines for Enablement of Government Departments for Adoption of Cloud

DISCLAIMER

This document has been prepared by Cloud Management Office (CMO) under Ministry of Electronics and Information Technology (MeitY). This document is advisory in nature and aims to provide information in respect of the GI Cloud (MeghRaj) Initiative.

Certain commercial entities, technology, or materials may be identified in this document in order to describe a concept adequately. Such identification is not intended to imply recommendation or endorsement by MeitY.

While every care has been taken to ensure that the contents of this Document are accurate and up to date, the readers are advised to exercise discretion and verify the precise current provisions of law and other applicable instructions from the original sources. It represents practices as on the date of issue of this Document, which are subject to change without notice. The readers are responsible for making their own independent assessment of the information in this document.

In no event shall MeitY or its' contractors be liable for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information) arising out of the use of or inability to use this Document

Table of Contents

Table of Figures

1. Purpose

This document is prepared to assist the Government Departments in easier understanding & navigating through the various standards, frameworks, guidelines, and templates on their way towards adoption of Cloud Services.

The document has primarily been segmented into 5 stages of Cloud Adoption and Enablement lifecycle viz. **Identification and Assessment, Planning, Build, Implement and Management & Monitoring.** These stages will assist Government Departments throughout the lifecycle of Cloud implementation from identifying the opportunity and assessing the Cloud readiness to the various facets of monitoring and management of Cloud.

2. Background

The Government of India has paved the way for mass adoption of Cloud services by the Government and Public sector organizations by empaneling the CSPs with Ministry of Electronics & Information Technology (MeitY). The CSPs are empaneled to offer Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) under the three Cloud Deployment models namely, Public Cloud (PC), Virtual Private Cloud (VPC) and Government Community Cloud (GCC).

With time, the Government Departments have started evaluating, planning, and adopting Cloud Services from the empaneled CSPs. As the adoption of technology within the Government Departments is evolving, it is intrinsic that the application workloads of the Government Departments are becoming complex in nature. Hence, it has become a prerogative for the Government Departments to evaluate and assess the Cloud readiness of their applications and migrate to a suitable platform to meet the ever-evolving technological demands. During this period, few of the Government Departments have also expressed their concerns over the lack of guidelines that could enable them to structure their Cloud adoption and migration strategy appropriately.

These issues make it imperative to develop certain guidelines around Cloud adoption and migration process which will assist the Government Departments in assessment of their existing IT platform, evaluating the right Cloud model and the suitable CSP for Cloud enablement of their IT workload(s).

3. Cloud Adoption and Enablement Lifecycle

Outlined in this document are keys stages to assist Government Departments in the adoption and implementation of cloud services and to ensure best practices, vital to success of their Department objectives. One of the key stages of Cloud Adoption and Enablement is the process of Migration.

3.1 Cloud First Approach of MeitY

With the advent of cloud in India, the country is ushering into an era of Digitalization. In 2013, MeitY published the document named as "GI Cloud (MeghRaj) Strategic Direction Paper" which provided a direction towards establishing and implementing the GI Cloud and an approach for its adoption by the government.

As a part of the MeghRaj initiative, MeitY came out with the **'Cloud First'** approach under which all the departments are required to assess and adopt cloud computing for their current as well as new applications. To further enhance this adoption, MeitY also empaneled Cloud Service Offerings of private Cloud Service Providers (CSPs) which could be availed by the Government Departments under this initiative.

Government Departments in India post MeitY's Cloud First approach have exhibited a positive advent towards cloud adoption. The focus of the Cloud First approach is to enable Government Departments to deliver both internal function and citizen centric services by leveraging cloud making cloud the default option.

By leveraging cloud, the Government Departments would be able to optimally use IT infrastructure leading to optimal spending on IT procurement, but this would also help them on focusing the core services of the respective department.

Cloud enables Government Departments to procure tools and technologies which are not feasible and viable to procure as a part of standard IT procurement. Every Government Department should adopt a '***Cloud-by-Default***' approach when designing a new IT service/ application or migrating or enhancing an existing application to reap both financial and non-financial benefits of cloud.

The plan for cloud adoption should be well identified by the Government Departments – whether their requirements are for short, medium, and long term. The Government Departments should be able to leverage the benefits of the cloud and integrate them into the existing infrastructure in an orderly manner. Cloud technology should be implemented or integrated into the IT infrastructure in such a way that it can be controlled and managed in a strategic manner. Government Departments must adopt a clearly defined strategy on using and managing the Cloud in order to be able to take advantage of the benefits offered.

3.2 Cloud Enablement Lifecycle

Migration of IT Infrastructure to Cloud is the process of moving application data and platform to the Cloud environment. Depending on the Government Departments requirement(s), the possibility of migration can be from an On-Premise environment to a Cloud Service Provider platform (On-Premise to Cloud Migration) or from one Cloud Service Provider platform to another Cloud Service Provider platform (Cloud to Cloud Migration).

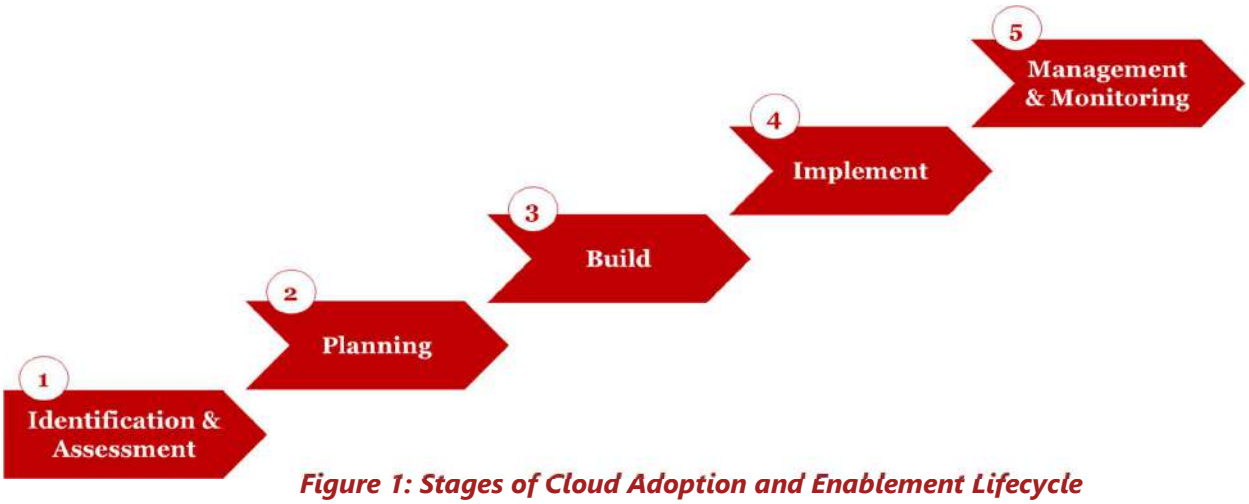
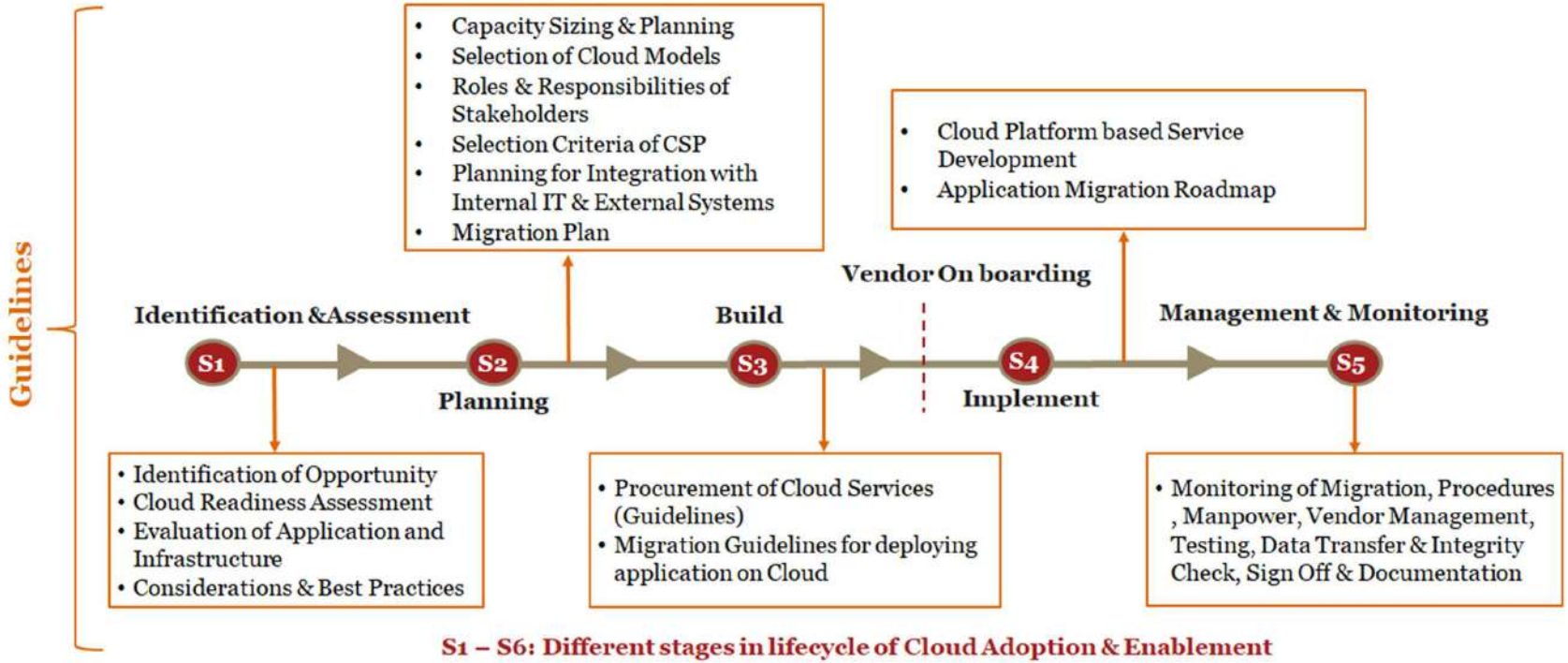


Figure 1: Stages of Cloud Adoption and Enablement Lifecycle

The below diagram depicts the stages of the involved in Cloud Enablement and Adoption lifecycle for a Government Department and the guidelines covered under each stage in this document, to enable Government Department for evaluation and migration to Cloud Services/ platform procured by them.

Figure 2: Cloud Enablement & Adoption Lifecycle



S1 – S6: Different stages in lifecycle of Cloud Adoption & Enablement

A holistic and meticulous upfront planning is needed before migrating Government Department applications to Cloud. Some common elements of a cloud migration strategy include evaluating performance and security requirements, calculating costs and making any necessary departmental changes.

Common challenges a department faces during a cloud migration include interoperability, data and application portability, data integrity and security, and business continuity. Without proper planning, a migration could negatively affect workload performance and lead to higher IT costs, thereby negating some of the main benefits of cloud computing.

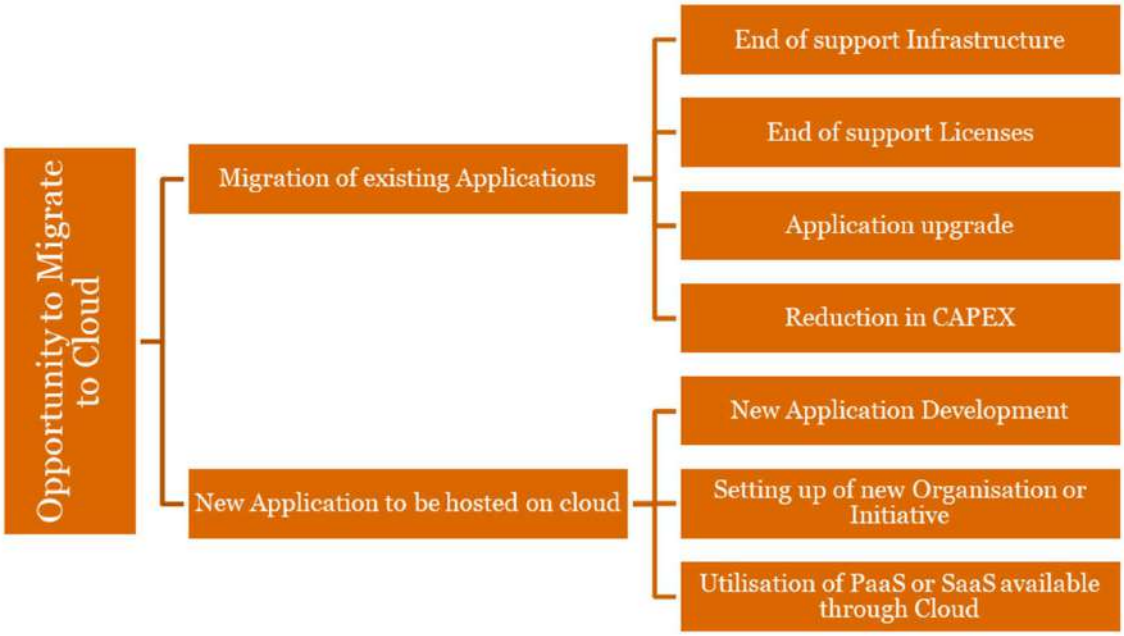
4. Stage 1: Identification & Assessment

With present advancements in technologies and MeitY's Cloud First approach the transitioning of Government Department's internal and citizen centric applications towards digitalization is becoming the need of the hour.

Government Departments planning for an update or refresh of their existing IT infrastructure (Hardware and Software) due to end of support, end of product lifecycle may refer to the section below, which shall enable them to identify possible opportunities available for adopting cloud. This section also details the process of evaluating applications and infrastructure on multiple facets in order to categorize and prioritize applications which can be readily be moved to Cloud and the applications which need changes and alterations to make them Cloud ready. Multiple factors that are involved in assessing applications have also been detailed in this section. The readiness of the application spans across various considerations, including, application and infrastructure, data and security, technology and integration, and business concerns. The guidelines outlined in the section below would assist Government Departments to identify and assess the suitability of applications for migrating them to cloud, along with the considerations and best practices which should be followed before planning a migration activity.

4.1 Identification of Opportunity

With inherent benefits of cloud being made available to the Government Departments it is subsequently important for the Government Departments to identify their requirements in Cloud and apparently initiate the process to adopt Cloud. By analyzing their business and IT objectives as well as current IT workloads housed either in their own Data Centers, NIC Data Centers, State Data Centers and CSP Data Centers, the Government Departments can identify relevant opportunities which make cloud adoption essential. The Government Departments may view the following as potential opportunities to migrate to cloud.



Some of the indicative factors influencing the adoption of Cloud by Government Departments are as follows:

(i) **Reduction in CAPEX***:* Infrastructure costs gets reduced considerably as the need to purchase expensive equipment and systems, maintenance and energy consumption costs, gets eliminated. It also reduces delays in service resolutions. Moreover, the pay-as-you-go model is more cost-efficient.

(ii) **New Application Developmen**t: The cloud enables greater business agility as it offers a platform for rapid development and deployment of new applications. Government Departments planning for new application development can opt for developing applications on Cloud. This can help Government Departments to have immediate access to the latest innovative business strategies.

(iii) **Setting up of new organization or initiative**: While planning setup of new IT infrastructure or new department altogether, it is recommended to setup Cloud environment as there are various advantages of opting Cloud over on-premises infrastructure. Some of them are mentioned below:

a) **Business agility:** Greater business agility is offered by Cloud as it offers a perfect platform for rapid development, deployment, and experimentation. Government Departments can have immediate access to the latest innovative business strategies.

b) **Scalability:** Cloud adoption makes it easier for Government Department to scale up or down according to their operation and storage requirements.

c) **Flexibility:** Cloud increases flexibility as Department users can access their data from anywhere. This boosts productivity

d) **Enhanced efficiency:** The cloud environment enhances work efficiency, offering seamless collaboration between various applications.

(iv) **End of Support Infrastructure & Licenses:** Government Departments facing end of support for infrastructure or licenses can opt to move on Cloud environment. These applications can be migrated to Cloud which will help in reducing the overall IT cost.

4.2 Cloud Readiness Assessment of an existing Application

Cloud Readiness can be defined as an activity to understand if the Government Department(s) IT work load (Application Stack) is ready to be deployed on Cloud or not. Cloud Readiness Assessment shall help provide a Government Department with clarity of vision and steps required to successfully adopt Cloud within their department. The said activity shall help a Government Department with a gap-analysis of their existing application landscape; Technical Feasibility, Risk Assessment, Strategic Alignment, and Cost Assessment in order ensure smooth migration.

The Existing application of a Government Department needs to be assessed categorically based on certain criteria, as listed below-

(i) Technical Feasibility Assessment
(ii) Risk Assessment (Refer Annexure 1)
(iii) Strategic Alignment and Cost Assessment (Refer Annexure 2)

Each of the above category has multiple dimensions defined in the document below. It is essential for a Government Department to assess the existing application on Technical Feasibility, ie. if the existing application is technically fit to be migrated on Cloud or if it needs Cloudification (making application Cloud ready). However, the Government Department may additionally assess their applications on Risk and Strategic criteria. The Cloud Readiness Assessment categories, dimensions, and guiding questions are indicative in nature and for guiding purpose only. They may or may not be applicable to the Government Department and the same may be amended as per Government Department requirements.

The various indicative dimensions across which an application may be assessed technically are:

(i) Application Dependency / Integrations
(ii) Network Sensitivity
(iii) Performance Needs
(iv) Recovery Capabilities
(v) Horizontal & Vertical Scaling
(vi) Technology Support
(vii) Security Requirements
(viii) Operational Availability
(ix) Monitoring

4.2.1 Technical Feasibility Assessment

The Technical Feasibility Assessment activity shall help a Government Department analyze its application on dimensions, such as Interdependency (dependency of application on different application, hardware, or platform), sensitivity to network, Horizontal & Vertical Scaling capability etc. Each dimension is defined in its description and guiding questions have been supplemented, which shall help the Government Department to objectively analyze the technical feasibility of application to be, migrate to cloud. Post performing the Technical Assessment with the guiding questions the Departments will be able to migrate to cloud with ease. Each dimension and its guiding question(s) may be modified by the Government Department according to their requirements.

Dimension	Description	Guiding Question	Response (Yes / No)
Application Dependencies/ Integration	The application in the existing environment may be dependent on any other application or hardware for it to run successfully. The application interface may be coupled with the complexity of interfaces to other applications (i.e. standard or custom UI components, external system integration, web service database controls)	• Is the application tightly coupled with other applications? • Does application have any specific hardware dependencies (e.g. Server, Storage, Firewall etc.) If the answer to all or any of the question(s) is 'No', the application should be easily migrated to Cloud If the answer to all or any of the question(s) is Yes, the Government Department should be able to migrate its application to Cloud by adopting following measures: • In case there are tightly coupled applications, Government Departments can migrate the entire stack of hardcoded interdependent applications together on cloud. • In case of any specific hardware dependencies, Government Department should procure the hardware components as a service from the empaneled Cloud Service Providers as feasible.	
Network Sensitivity	The applications running in the existing environment may be dependent on the internal & external Network on which it is running and	• Is the application dependent on certain proprietary network components (such as Switches, Routers, VPN clients etc.) using proprietary protocols?	

Dimension	Description	Guiding Question	Response (Yes / No)
	high sensitivity to network may lead to performance impact. Separation of the application tiers (e.g. web, application, middleware, and database) for transactions is susceptible to performance degradation due to latency.	• Is the application transporting large amount of data over the network? If the answer to all or any of the question(s) is 'No', the application should be easily migrated to Cloud If the answer to all or any of the question(s) is Yes, the Government Department should be able to migrate its application to Cloud by adopting following measures: • In case of any specific proprietary network components, Government Department should procure the components as a service from the empaneled Cloud Service Providers as feasible. • In case the application transports large amount of data over the network, Government Department may use connectivity options such as Point to Point link, MPLS, Site to Site VPN etc. provided by the CSP.	
Performance Needs (User Experience)	Application performance needs in terms of Response Target Times. Application is required to perform at the desired level in the event of changes to the workload (e.g. DC location, end point infrastructure, connectivity)	• Does the performance needs of application change with location of users? • Is the application and its associated database regularly optimized / modified in the current environment? If the answer to all or any of the question(s) is 'No', the application should be easily migrated to Cloud If the answer to all or any of the question(s) is Yes, the Government Department should be able to migrate its application to Cloud by adopting following measures: • In case application performance needs change with location of users, the Government Department may use cloud services such as CDN for optimizing performance.	

Dimension	Description	Guiding Question	Response (Yes / No)
		• The Government Departments may migrate a non-optimized application to cloud. Employing optimization may allow Government Departments to leverage the pay per use feature of cloud.	
Failover Capabilities	Failover capabilities define the ability of system or application to recover in case of unseen abnormalities in system behavior (downtime, application unresponsiveness).	• Does the Application not have failover capabilities? If the answer to all or any of the question(s) is 'No', the application should be easily migrated to Cloud If the answer to all or any of the question(s) is Yes, the Government Department should be able to migrate its application to Cloud by adopting following measures: • In case the Application does not have failover capabilities the Government Department may leverage the auto scaling feature of cloud as a part of the architecture.	
Horizontal & Vertical Scaling	The ability of application to scale horizontally and vertically to cater to spontaneous increase in traffic, sudden burst/peak in application accessibility etc.	• Is the application running in traditional IT environment (physical IT hardware with no virtualization)? • Does application experience abrupt increase in utilization (e.g. peaks during Quarters end or month end or specific periods as per Government Departments application nature)? • Does the Application Architecture need modification to natively support vertical / horizontal scaling (load balancing across dynamically provisioned computing resources)? If the answer to all or any of the question(s) is 'No', the application should be easily migrated to Cloud	

Dimension	Description	Guiding Question	Response (Yes / No)
		If the answer to all or any of the question(s) is Yes, the Government Department should be able to migrate its application to Cloud by adopting following measures: • In case the application is running in a non-virtualized environment, the Government Department may migrate the application to cloud but pay close attention to the resource requirement on cloud post migration. • In case the application experiences abrupt increase in utilizations over a period, the Government Departments may employ horizontal or vertical scaling feature of the cloud to handle such bursts. • The Government Department post migration to cloud may leverage Horizontal Scaling incorporating it in the application architecture but in case of vertical scaling the application may need to be analyzed for using or supporting the feature.	
Technology Support	Applications running on legacy platforms that are not supported or would need specific contracts with CSP / MSP to support.	• Does your application run on legacy platform or OEM specific platforms (Hypervisors), which currently needs specific extended support contracts? (e.g. cannot run on x86 platform or supported OS platform) • Does application need re-write or re-factoring to natively support various CSP services? If the answer to all or any of the question(s) is 'No', the application should be easily migrated to Cloud If the answer to all or any of the question(s) is Yes, the Government Department should be able to migrate its application to Cloud by adopting following measures:	

Dimension	Description	Guiding Question	Response (Yes / No)
		• The Government Department may need to modify the application to be able to host it on updated OS currently supported on the cloud. • In case Government Department wants to use certain services natively from the cloud the Department may choose an As a Service offering of the cloud. The application may be needed to redesign as per feasibility to natively support various CSP services.	
Security Requirements	The application security requirements and ability of Cloud provider to meet the requirements	• Does the application work on hard coded IPs? • Does the Government Department need isolated environment and dedicated security components for security reasons? If the answer to all or any of the question(s) is 'No', the application should be easily migrated to Cloud If the answer to all or any of the question(s) is Yes, the Government Department should be able to migrate its application to Cloud by adopting following measures: • If the application works on hardcoded IPs, the Government Department may redesign the application to remove dependencies on hard-coded IPs and migrate the application to cloud. • In case a Department needs dedicated security components along with an isolated environment exclusive for Government Cloud consumers, the Department may evaluate Government Community cloud (GCC) for its requirement and migrate to cloud.	

Dimension	Description	Guiding Question	Response (Yes / No)
Operational Availability	The change in operations for the particular application (i.e. maintenance, administration, SLA requirement)	• Is the Government Department using SLA parameters currently unavailable with the CSPs? • Does moving to cloud increase the complexity of managing the application (due to multiple application vendors for the department) which may impact SLA requirements? If the answer to all of the question(s) is 'No', the application is technically feasible to migrate to Cloud. If the answer to all or any of the question(s) is Yes, the Government Department should be able to migrate its application to Cloud by adopting following measures: • Post migration to cloud the Government Departments may leverage use of SLA tools available on cloud and designing custom parameters on the same if feasible. • For migration to Cloud the Government Department may evaluate a Managed Service Provider (MSP) who shall co-ordinate with multiple App vendors of the Department and ensure management of the Department's cloud.	
Monitoring	Application Monitoring of the application and its parameters which would allow Government Department to leverage and scale / optimized the cloud resources.	• Is Application level monitoring performed for the application and associated databases? • Do you currently leverage custom or specific KPI's for scaling / optimizing the application? If the answer to all or any of the question(s) is 'No', the application should be easily migrated to Cloud. If the answer to all or any of the question(s) is Yes, the Government Department should be able to migrate its application to Cloud by adopting following measures:	

Dimension	Description	Guiding Question	Response (Yes / No)
		• In case Departments use Application Level Monitoring, the Government Departments may evaluate system monitoring/ Infrastructure monitoring tools (EMS tools) available on the cloud platform as a service for monitoring various metrics. • Post migration the Government Departments may implement a customized EMS tool on cloud to monitor specific KPIs/ metrics required by the Department.	
Identity Management	The identity management capabilities leveraged by the application to manage Access control (authentication, authorization) and privileges within or across system and Government Department boundaries to secure sensitive data and be compliant with regulatory mandates.	• Does the application leverages centrally managed identities for authentication, authorization, provisioning and de-provisioning access to the application & it's components? • Is the Government Department currently using OEM specific IAM tools or modules? If the answer to all or any of the question(s) is 'No', the application should be easily migrated to Cloud If the answer to all or any of the question(s) is Yes, the Government Department should be able to migrate its application to Cloud by adopting following measures: • The Government Department may evaluate compatible IAM tools on cloud, use of centralized Active Directory or Identity and Access Management Software on cloud and migrate their workloads to cloud.	

4.3 Identification and Evaluation of Application and Infrastructure

The complexity of an application is determined by its nature and dependencies on other applications and processes. Applications with lesser dependencies on other applications or external systems or having a low risk profile tend to be easier to migrate. To identify and evaluate the applications and infrastructure, Departments may go through the following section which will guide them in performing Application and Infrastructure Assessment

4.3.1 Application Portfolio Assessment

1 **Create Application Inventory:** Government Department should inventorize all software applications and their versions, as it is required to properly plan and gauge the complexity of the migration. Understanding the criticality of each application to the department, departments should inventorize each deployment environment, including development, application testing, integration, user acceptance testing, staging, and production environments.

2 **Identify Application Interdependencies:** Next step is to identify interdependencies between applications. Applications with low-complexity and have minimal or no dependencies can be migrated preferentially. Then departments can move on to high-complexity applications that may be running on legacy OS, mainframes, or that may have related components that need re-licensing.

3 **Application Prioritization, complexity and Risk Model:** Departments should prioritize their migration strategies based on the criticality and the associated risks of applications. For applications which have low-risk environments like development and testing typically go first, followed by development and test environments and finally, high-risk production environments.

4 **Infrastructure Assessment:** After assessing the various aspects of applications to be migrated, it is important to assess the Infrastructure of the Cloud Service Provider (CSP) where application to be migrated is located. The major aspects in Infrastructure assessment are:

5 **Identify Networking bandwidth, Connectivity:** Departments should ensure a secure network connectivity between it office locations as well as the proposed Cloud platform. VPN is considered to be the most secure form of connectivity and can decrease vulnerability exposure. It provides layered security throughout to ensure data and connections are properly protected.

6 **Identify Compute/Server, Storage:** While analyzing the infrastructure, departments should also assess the current compute storage and database capacity consumed by the existing servers. To analyze the available compute/server and storage, departments can use following factors:

Server:

- Server type
- Number of virtual machines
- CPU cores
- Memory in GB
- Server types: Hypervisor, Guest OS, and DB Engine
- Utilization for CPU, Memory & Disk

Storage:

- Storage Type
- Raw Storage Capacity
- Percent Accessed Infrequently (Object Storage)
- IOPs
- RAID Level

After identifying the above factors, departments can also analyze the current utilization and size match in cloud

7 **Analyze current utilization and size match in Cloud:** It is important to analyze the capacity requirements of applications to be migrated. Key metrics to consider for understanding requirements include peak CPU utilization, allocated and peak RAM usage, and usage patterns.

8 **Peak Utilization: I**t is important to identify peaks in CPU & memory usage. Assessing average workloads instead of peak can give less accurate prediction of usage which may cause infrastructure to suffer serious performance degradation when peak hits.

4.4 Considerations/Best Practices for Cloud Adoption & Migration

This section details about the considerations and best practices which may be adopted before planning migration to Cloud environment. It also details the factors which should be considered while migrating to Cloud, such as security, transition process, Service level Agreements, and Financial & Legal aspects.

4.4.1 Considerations

The section lists out essential factors which may help Government Departments to make appropriate and thoughtful decisions before planning the Cloud migration.

The below diagram explains the key considerations for Cloud Adoption and Enablement Lifecycle

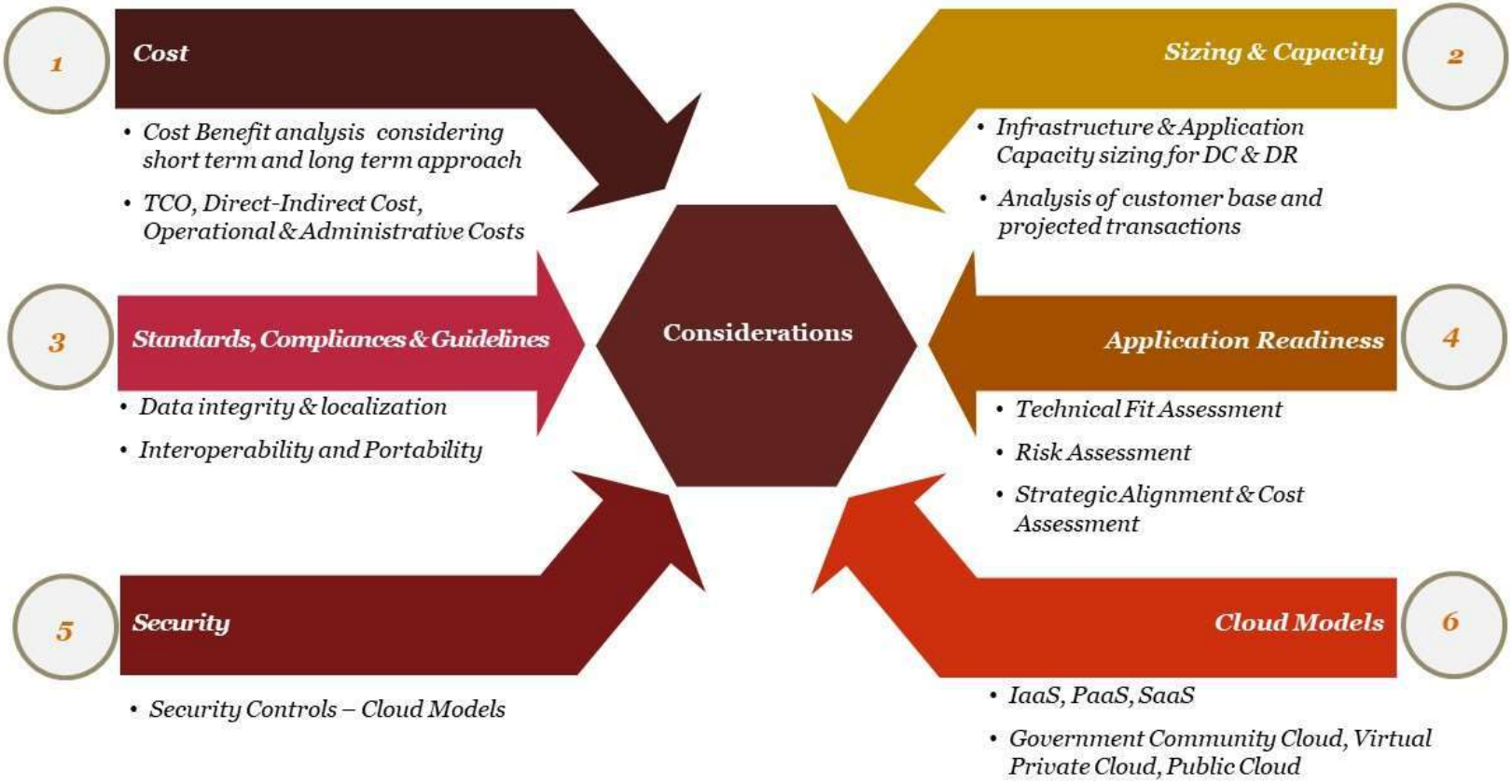


Figure 3: Key Consideration for Cloud Adoption & Migration

1 ***Cost:*** Government Departments should adopt a holistic approach while calculating the total cost of migration from on-premises to Cloud environment or from one CSP environment to another CSP environment. While, Cloud offers lower costs, but there are various factors that should be considered such as, direct costs, operational costs, administrative costs and indirect cost. It is also necessary to consider the transition period during which departments will be incurring cost for on-premises data center as well as cloud.

Total Cost of Ownership (TCO) is also one of the important factors that needs to be accounted before planning migration. The calculations for TCO are generally based on the assumption that cloud computing doesn't require major hardware/software investments upfront and the Departments only pay for the resources they actually use/consume.

2 ***Capacity Sizing:*** The Capacity Sizing of compute, storage, network, and connectivity require analysis of present utilization of the existing Infrastructure & applications and future growth in terms of transactions and user base. Identifying the optimal resources required in the cloud for each of the workloads shall enable Government Departments to achieve optimal performance requirements and shall allow upsizing and downsizing of resources as per requirement. The Capacity Sizing guidelines can be referred from Section 5.1 'Guidelines for Capacity Sizing'.

3 ***Standards, Compliances & Guidelines:*** During the evaluation of a CSP by the Government Departments one of the key features which govern the decision of migration is interoperability and portability. This ensures Government Departments have the ability to move applications from one CSP to another with minimum changes possible and adopting commonly used formats for importing data into procured CSP Platform. For Government Departments migrating their IT workloads especially sensitive data, it is pertinent to When the Government Departments plan migration to Cloud, a detailed analysis of an application is performed to assess its Cloud readiness. Some of the existing applications may need modernization to take the advantage of the cloud. Government Departments can refer the Cloud readiness assessment guidelines Section 4.2 of this document and ensure that the data stored in any device on the Cloud needs to be present within the borders of the Country.

4 ***Application Readiness:*** When the Government Departments plan migration to Cloud, a detailed analysis of an application is performed to assess its Cloud readiness. Some of the existing applications may need modernization to take the advantage of the cloud. Government Departments can refer the Cloud readiness assessment guidelines Section 4.2 of this document.

5 ***Security:*** Implementation of well-defined security policies & procedures is a must for ensuring adequate security of the applications in the cloud. Migrating infrastructures, services or applications to the cloud without increasing the security overhead requires vigilant preparation & strengthening of security posture. Successful cloud migration

requires migrating security to the cloud enabling Government Departments to deploy and manage a single, consistent security framework that covers the complete Cloud infrastructure.

6 ***Cloud Models:*** Government Departments must understand how the Cloud architecture and Platform line up with their current environment and see the dependency of components. The evaluation of Cloud Service & Deployment Model is an essential step towards Cloud migration. For more details, Government Departments can refer guidelines on Cloud Deployment and Service Models, Section 5.2 of this document.

4.4.2 Best Practices

When departments plan for Cloud migration, various processes and practices may be evaluated during the planning stage for implementing a successful cloud-migration strategy. Though every cloud migration event has unique set of requirements, few common best practices help Government Departments in successfully migrating to cloud.

1 **Data Backup during Migration:** While performing application migration it is pertinent to ensure the protection of Government Department's data. It is proposed that Government Departments always create a full backup of their systems which they plan to migrate before performing the actual migration. Any unexpected event during migration may result in loss of data or unusable application state. Hence, backup gives an extra layer of protection in such events.

2 **Formulate a properly planned migration strategy:** Government Departments should begin the migration process by mapping out a migration strategy that identifies clear business motives and use cases for moving to the Cloud.

3 **Manage the software licensing:** A major concern for Government Departments is whether their existing licenses for on-premises software can be extended to Cloud. Hence, Government Departments can leverage on the Bring Your Own License (BYOL) program that give Departments the flexibility to reuse their licenses on Cloud.

4 **Prioritize Migration Dependencies:** Before migrating to Cloud, during the planning stage it is important to identify the dependency of each component or services and their connections. For the Government Departments having complex on-premises setups, it is a good practice to understand dependencies of various workloads and prioritize migration of workloads with minimum to maximum dependencies accordingly.

5 **Roles & Responsibilities:** Charting out complete Roles & Responsibilities of stakeholders, customized to the Government Department Project requirements

5. Stage 2: Planning

Once the Identification and the Assessment stage has been completed, structured planning is required by the Government Departments to adopt cloud, which includes understanding the criteria for evaluating the CSPs, performing the capacity sizing estimation for Compute, Storage and Network and selection of Cloud models suitable for migrating their existing applications. Various roles and responsibilities of Stakeholders involved in the process of migration have also been explained in this section.

5.1 Guidelines for Capacity Sizing

A key area during the lifecycle and particularly planning of migration activity is Capacity Sizing. The amount of compute, storage, and network bandwidth, connectivity required can be estimated by performing capacity sizing of the existing Infrastructure and applications. Every Government Department, planning to migrate its existing applications or any new application to be deployed on Cloud, is required to do capacity sizing to estimate the actual amount of resources required on Cloud. Identifying the optimal compute and storage resources in the cloud for each of the workloads shall enable the Government Department to achieve maximum performance requirements at the lowest possible cost.

The key to right sizing is to understand your department usage needs and patterns and know how to take advantage of the elasticity of the Cloud to meet those needs.

This section of the document defines the guidelines and approach that may be adopted by a Government Department while carrying out Capacity Sizing of the Compute, Storage and Network.

S. No	Sizing Parameters	Traditional	Compute (Cloud)	Storage (Cloud)	Network (Cloud)	Security (Cloud)
Infrastructure as a Service						
1.	**Redundancy**	• Need to procure physical server, storage, network and deploy it to achieve redundancy	• Additional VMs can be added to achieve redundancy through clustering and load balancing • May result in additional cost	• CSPs provide multiple storage copies at different locations to store the data and keep it safe (Geo Resiliency) • Can also be procured as a service and charges to be in accordance	• Core Network components natively provided as an inclusive service by the Cloud Service Provider	• Subjective to Government Departments requirements, the department may procure security services in redundancy to meets its requirements
2	**Performance**	• Capture CPU and Memory utilization for a period of 3 months to 1 year	• Capture CPU and Memory utilization for a period of 3 months to 1 year including peak utilization periods • This data can be further analyzed and used to draw performance patterns • Threshold limit of 70% - 80% can be pre-configured for alerts	• Capture storage utilization along with IOPS consumption for a period of 3 months to 1 year • This data can be further analyzed and used to draw performance patterns • Threshold limit of 70% - 80% can be pre-configured for alerts	• Capture utilization pattern for existing network components and resources for a period of 3 months to 1 year • This data can be further analyzed and used to procure required Network services on Cloud such as bandwidth	• Assessment of existing security components and their utilization pattern can help decide security services to be procured on Cloud.
3.	**Scalability**	• Achieving scalability in traditional environment is a cumbersome task and needs addition of	• The compute environment on Cloud with inherent functionality of virtualization can be scaled up to the level supported by underlying H/w & S/w	• The storage on cloud is virtualized to derive maximum benefit and share the same among the compute resources / users • Additional storage can be added as partition to	• The N/w components required on cloud shall be available as a service and the CSP providing the services shall scale	• The Security components shall be dedicated to or made available as a service to Government Department and the service can be scaled

		physical IT resources (Servers, Network, Storage, Security etc.)	• Additional resources can be added on virtual machines to achieve more scalability	meet additional storage needs and providing scalability	it to the level required • To meet increasing demand the bandwidth provisioned can be scaled to a level (Burstable) to support optimal performance of the application	up or down by the CSP as per requirement
4.	**Availability**	• Achieving high availability in Traditional environment shall require deployment of additional physical IT resources and maintaining SLA, carrying out periodic maintenance	• The resources compute environment available on cloud can be configured in high availability mode with the help of clustering & load balancing	• Multiple copies of Data sets are stored on various storage using appropriate technology which can help achieve high availability	• The network components provisioned by the CSP as a service are natively made highly available in nature	• The security components are provisioned by the CSP as a service which can be made highly available using appropriate failover mechanism
5.	**Disaster Recovery**	• Separate physical Data Center setup needs to be provisioned and managed for meeting the Disaster Recovery	• The compute on Cloud-DR, can be made available and run with minimum resources and can be scaled up in case of actual disaster	• To achieve complete replication of data and maintaining one copy of data on DR site, the storage shall be replicated 100% and shall be sized accordingly to maintain the data at DR site	• Providing N/w components at DR site shall be in scope of the CSP and it shall be responsibility of CSP to ensure network configuration at DR	• Providing Security components at DR site as per Government Department requirements shall be in scope of the CSP and it shall be responsibility of CSP to ensure configuration at

		requirements, which is a complex and costly activity			similar to that of DC site	DR similar to that of DC site though the Government Department may choose security components to be in standalone mode in DR
Platform as a Service						
1.	**Redundancy**	With Procurement of additional physical IT Infrastructure along with license for platform	• Additional VMs can be added to achieve redundancy through load balancing • The CSP shall be responsible to maintain redundancy for platform provided to the Government Department as per requirement	• The storage service provided as platform by the CSP shall be provisioned with redundancy while providing service to the Government Department	• Network components natively provisioned as a service with availability as per SLA, defined by MeitY and Government Department	• Security Components provided as a service may be offered with redundancy as per requirement
2.	**Performance**	Capture compute, storage and N/w utilization, appropriate tools would need to be in place for evaluating performance of middleware etc.	• Capture CPU and Memory utilization for a period of 3 months to 1 year • This data can be further analyzed and used to draw performance patterns and accordingly platform service can be provisioned to meet performance requirements	• Capture storage utilization for a period of 3 months to 1 year • This data can be further analyzed and used to draw performance patterns	• Capture utilization pattern for existing network components and resources for a period of 3 months to 1 year • This data can be further analyzed and used to procure N/w services such as bandwidth on Cloud.	• Assessment of existing security components and their utilization pattern can help decide security services to be procured on Cloud.

					• The configuration of N/w components shall be in CSPs scope	
3.	**Scalability**	Not Applicable	• Scalability of compute required shall be complete responsibility of the CSP to meet the Government Department requirements	• Scalability of storage required shall be complete responsibility of the CSP to meet the Government Department requirements	• Scalability of network resources required shall be complete responsibility of the CSP to meet the Government Department requirements	• Scalability of security required shall be complete responsibility of the CSP to meet the Government Department requirements
4.	**Availability**	Not Applicable	• Ensuring continuous availability of Compute resources shall be in scope of CSP through appropriate measures	• Provisioning of storage with high availability shall be in scope of CSP	• Ensuring high availability of N/w services procured by the department shall fall under CSPs purview	• High availability of security services shall be responsibility of the CSP • The Government Department may procure security services as per their requirements & complexity of the project
5.	**Disaster Recovery**	Not Applicable	• CSP shall be responsible to ensure services procured under platform as a service model are available for use even during any impact of disaster from DR site			
Software as a Service						
1.	**Redundancy**	Not Applicable	• The CSP shall be responsible to maintain redundancy of all the resources to provide any software as a service			

2.	**Performance**	Not Applicable	• The CSP shall take all adequate measures to meet performance requirements of a Government Department when providing software as a service
3.	**Scalability**	Not Applicable	• The scalability of services procured under SaaS shall be CSPs responsibility
4.	**Availability**	Not Applicable	• The CSP shall ensure the cloud services are running in high availability to avoid any impact on business operations
5.	**Disaster Recover**	Not Applicable	• The CSP shall be responsible for running all services procured under Software as a Service to keep the services running in case of any disaster

5.1.1 Capacity Sizing for Compute

Compute Services are the most essential services procured on Cloud. The basic unit of compute on Cloud is termed as a Virtual Machine, which shall be required to host and run an application, database server, Backup Server, Monitoring Server etc. The capacity sizing of compute services is required to be carried out to identify the actual quantity of Compute services that shall be procured by a Government Department to host its application on Cloud and to estimate the cost that may be incurred.

Below are the underlying factors that a Government Department should consider when carrying out Capacity Sizing.

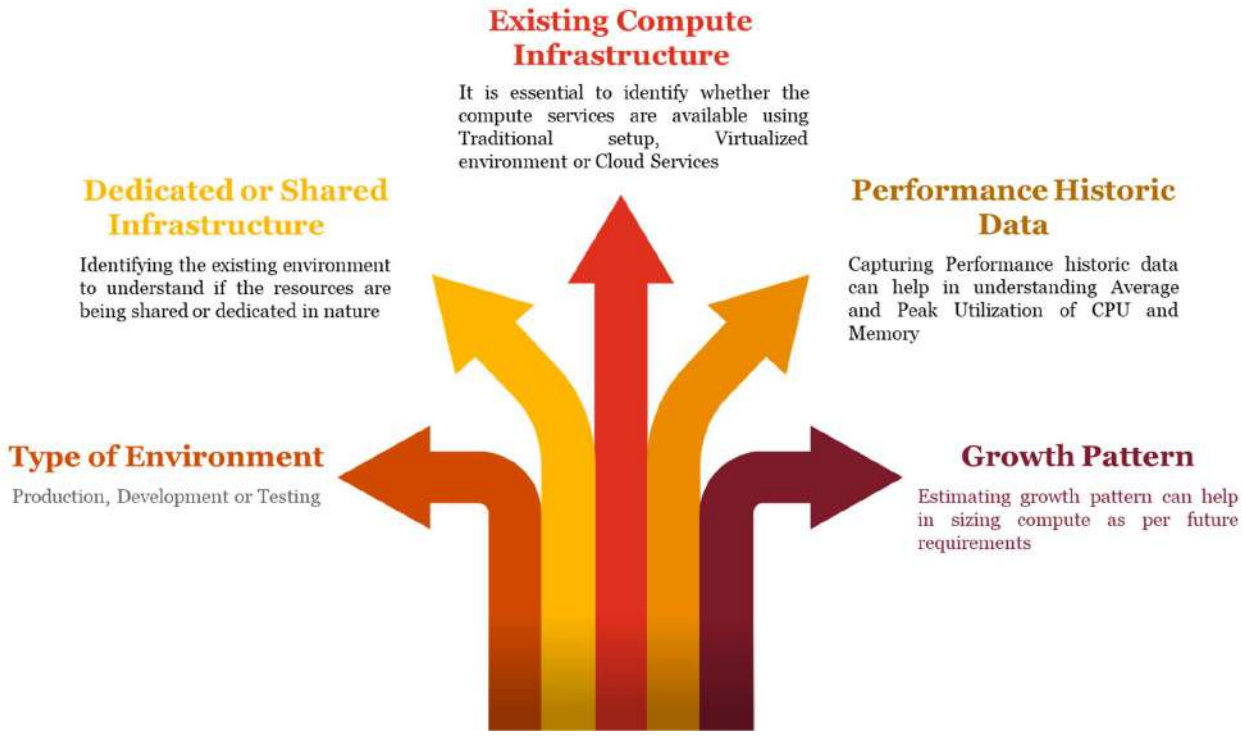


Figure 4: Factors for Capacity Sizing in terms of Compute

1 **Existing Compute Infrastructure:** The initial step for a Government Department is to gather information of existing compute environment and configurations, whether it is a traditional, virtualized on premise or a cloud set up. Gathering this data first hand shall assist the Government Department to understand the working and utilization of the existing environment, the licenses (Operating System, Database, Middleware, Security etc.), if the application is utilizing dedicated physical cores or virtualized cores and if the optimum performance is being achieved with such a configuration

2 **Dedicated or Shared Infrastructure:** Analysis of the existing infrastructure and understanding if it is dedicated or shared, shall help a Government Department analyze the actual resources required to meet compute requirements to run the applications in their environment.

3 **Type of Environment:** The Government Department should carry out assessment of the current setup and identify different environments (Production, Dev, Test, QA) in which various applications are running. Keeping in view the nature of the applications running in these environments it becomes pertinent to categorize and identify such applications which can be migrated on the fly along with other applications which might have interdependencies. Based on severity and criticality of the Government Department environments, performance measures and KPIs need to be identified and post deliberation on the same, migration activity can be streamlined.

4 **Performance Historic Data / Utilization based Historical Performance** A critical step in capacity sizing and management is to gather / import metrics for existing performance, capacity, and configuration for all the applications and resources currently running in the environment. The Government Department may capture data for average and peak CPU and memory utilization along with I/O statistics such as network throughput, disk throughput, and latency for a period of 3 months to 1 year. This data can further analyzed and used to draw usage and performance patterns and understand if equal configuration as per existing configuration of servers / VMs is required on cloud. An approximate threshold limit (such as 70% or 80% CPU utilization) as per existing usage trend can also be decided and configured when migrating to Cloud. On analyzing the performance metrics, the Government Department may identify that CPU utilization is below normal, but memory utilization is high, which indicates that an application may be Memory intensive. In such a scenario, the Government Department may opt for minimum compute required to run the application seamlessly without affecting its performance and opting for additional memory (RAM) with no change in compute when procuring virtual machine thereby optimizing Cloud deployment

5 **Growth Pattern:** On capturing and analyzing the performance data of applications and servers, the Government Department can identify the growth pattern in terms of the compute, memory, no. of users, load-balancing requirements. The metrics and data captured can further be analyzed to identify if an application is to be load balanced or if only increasing the compute and memory of the server on which it is running shall suffice the purpose. The growth pattern shall further help department to understand at what time intervals the need of adding more resources shall occur to continue running the application seamlessly.

The increase in

- Number of users
- Number of sessions
- Peak Page Throughput required (Peak number of pages / second requested by users)
- Page Cache Hit rate (number of page definitions that can be retrieved from the cache compared to the number of pages that must be regenerated during peak load times)

- Peak Login Rate (the rate at which users' login to the application server, thereby placing a load on the server)
- Page Load time (average amount of time required to load a page)

It may also help the Government Department in carrying out the optimum sizing of resources when migrating to Cloud and these metrics can also be used by the Government Departments after migration to get maximum benefits in terms of performance and cost.

When, carrying out this exercise the Government Department shall be in a better position to understand the existing architecture, performance criteria of the applications, identification of compute and or memory intensive applications, the requirement for load balancing and clustering and over provisioning, that can be done, without affecting performance of applications on Cloud. This overall activity may also help Government Department to do consolidation of servers, which shall further be helpful in deciding which servers or applications are not required to be migrated and which application(s) can share compute resources while meeting performance requirements.

5.1.2 Capacity Sizing for Storage

The Storage services form a key component when procuring compute service on Cloud, as the data that must be processed using compute services is required to be stored on a storage disk. When carrying out capacity sizing for storage, it may be categorized broadly in terms of the capacity and performance. Capacity refers to the amount of Data that can be stored on a disk and performance may be referred as IOPS (i.e. how quickly data can be read or written) and Latency (how long it takes to process a single request). The capacity sizing of storage services is required to be carried out to identify the actual quantity of storage and type of storage services that shall be procured by a Government Department to host its application on Cloud and to estimate the cost that may be incurred and to meet the overall solution requirements.

Below are the key factors that a Government Department may consider when carrying out Capacity Sizing for Storage.

1 Storage must be configured with enough disk drives to meet the IOPS and latency needs of the applications
2 When carrying out sizing for storage required on Cloud, the Government Department must consider the type of data that is proposed to be stored on the disk and also factor in the 'compression' and 'de-duplication' (if available)
3 The Government Department must identify and segregate the type of work load in accordance with Production / Development / Test Environment and performance needs
4 The Government Department may opt for SSD / Flash disks, SAS, SATA /NL-SAS as per the type of data that is to be stored and accessed for e.g. SSD / Flash drives shall offer highest performance in terms of high IOPS requirements
5 The Government Department may define the IOPS requirements and storage capacity specific to application and associated databases performance needs.

6 The Government Department may opt for 20% buffer when procuring Storage on Cloud to meet increasing demand

7 Storage infrastructure should be organized such that it is efficient enough to upgrade and add capacity to take care of any additional performance requirements.

8 Flash drives may be considered and sized for high transaction databases, roll-back segments and frequently accessed tables, frequently accessed Web content, applications with high random read requirements, business-critical applications impacted by low cache read hit rates.

5.1.3 Capacity Sizing for Network & Security

Network and Security capacity planning involves

- Structuring the network from the perspective of Utilization, Capacity, Operations, availability and other network constraint
- Sizing the Security components from the perspective of Throughput, User Count, Bandwidth, Transactions per second and other security constraints

Below are the key factors that a Government Department may consider when carrying out Capacity Sizing for its network and security infrastructure:-

1 For assessment of network components required to be procured on Cloud, the key task is to understand and analyze the current network traffic volumes.

2 It is essential for the Government Departments to understand the current network utilization patterns to cater to the increase in traffic and bandwidth requirement for procuring network services accordingly

3 If the Government Department currently has multiple connectivity options such as, MPLS, VPN, Point to Point, Internet Leased Line, in its infrastructure setup, then the Government Department should adopt adequate measures in order to support the same connectivity options when migrating to Cloud Service Provider platform (positioning of MPLS router, Port termination facilities available with CSP)

4 Assessment of Government Department current security posture, including but not limited to Firewalls, IPS, IDS, HIPS, Antivirus, SIEM, End Point Protection, DLP, DDoS protection and mitigation

5 Government Department must ensure equivalence to current and future security requirements while carrying out capacity sizing to migrate to Cloud.

6 This analysis shall help the Government Department to understand the amount of N/w & security resources needed to cater to the future requirements

5.2 Guidelines for Selection of Cloud Models

The evaluation and selection of Cloud Service Model is a key activity for any Government Department to conduct before selection of Cloud Services and the Cloud Service Provider. The three Cloud Service Models namely, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS) have various activities and responsibilities either managed by the Government Department (i.e. self-management) or managed by a MSP (i.e. managed by a Managed Service Provider). The below diagram depicts the key activities and delineates responsibility of the Government Department and the Managed Service Provider in each Service Model, which may help the Government Department to decide which service model should be selected and accordingly the Cloud Services may be procured

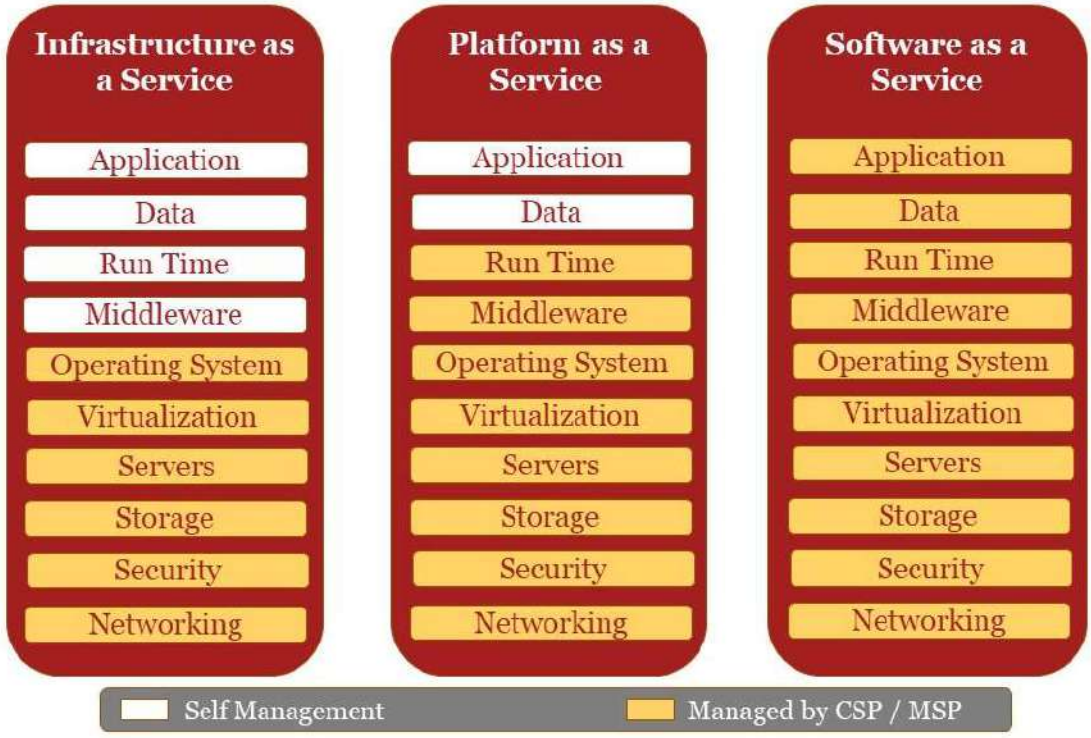


Figure 5: Cloud Service Models

1 **Infrastructure as a Service (IaaS):** The Cloud Service Provider is responsible to the Government Department with compute, storage, networks, and other fundamental resources where the Government Department is able to deploy and run arbitrary or standard 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 Government Department.

2 **Platform as a Service (PaaS):** The CSP shall provide the Government Department 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 Government 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.

3 **Software as a Service (SaaS):** The CSP shall offer a plethora of applications running on the its Cloud infrastructure as services to Government Departments. 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 Government 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.

The selection criteria for identification and adopting Cloud Service Model may be undertaken by the Government Department based on Technical and Regulatory parameters, as defined below in the table.

Category	Parameter	Infrastructure as a Service	Platform as a Service	Software as a Service
Technical	**Government Department Control**	Highest (Control lies with User)	Medium	Low
	Disaster Recovery	User shall be required to define DR requirements	User shall be required to define DR requirements	CSP shall define DR requirements and cycle (CSP responsible for application)
	Competency Required	High (Government Department needs to have highly technical competent resources	Medium	Low (CSP managed resources)
	Implementation Time	High	Medium	Low (ready to consume)
	Integration Feasibility	High	Medium	Low (subjective to integration methodologies)

Category	Parameter	Infrastructure as a Service	Platform as a Service	Software as a Service
Regulatory	**Forensic & Audit**	Can be conducted by Government Departments	Can be conducted by Government Departments	Can be conducted by CSP only
	Governance	High	Medium	Low
	Vendor Lock-in	Least	Low - Medium	High
	Cost (Indicative)	High	Medium	Low

5.3 Roles & Responsibilities of Stakeholders

Defining scope of services and responsibilities of each stakeholder such as Cloud Service Providers, Managed Service Providers, System Integrator (Implementation agency), and Government Department is a key activity for proper delineation of roles and responsibilities of each stakeholder.

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 for the Government Departments, improved process management, and enhanced operational performance.

Further, this section of the document covers Roles & Responsibilities of different stakeholders: -

1. Cloud Service Provider
2. Managed Service Provider
3. System Integrator / Implementation Agency
4. Government Department

The key responsibilities of the above-mentioned stakeholders are highlighted below:

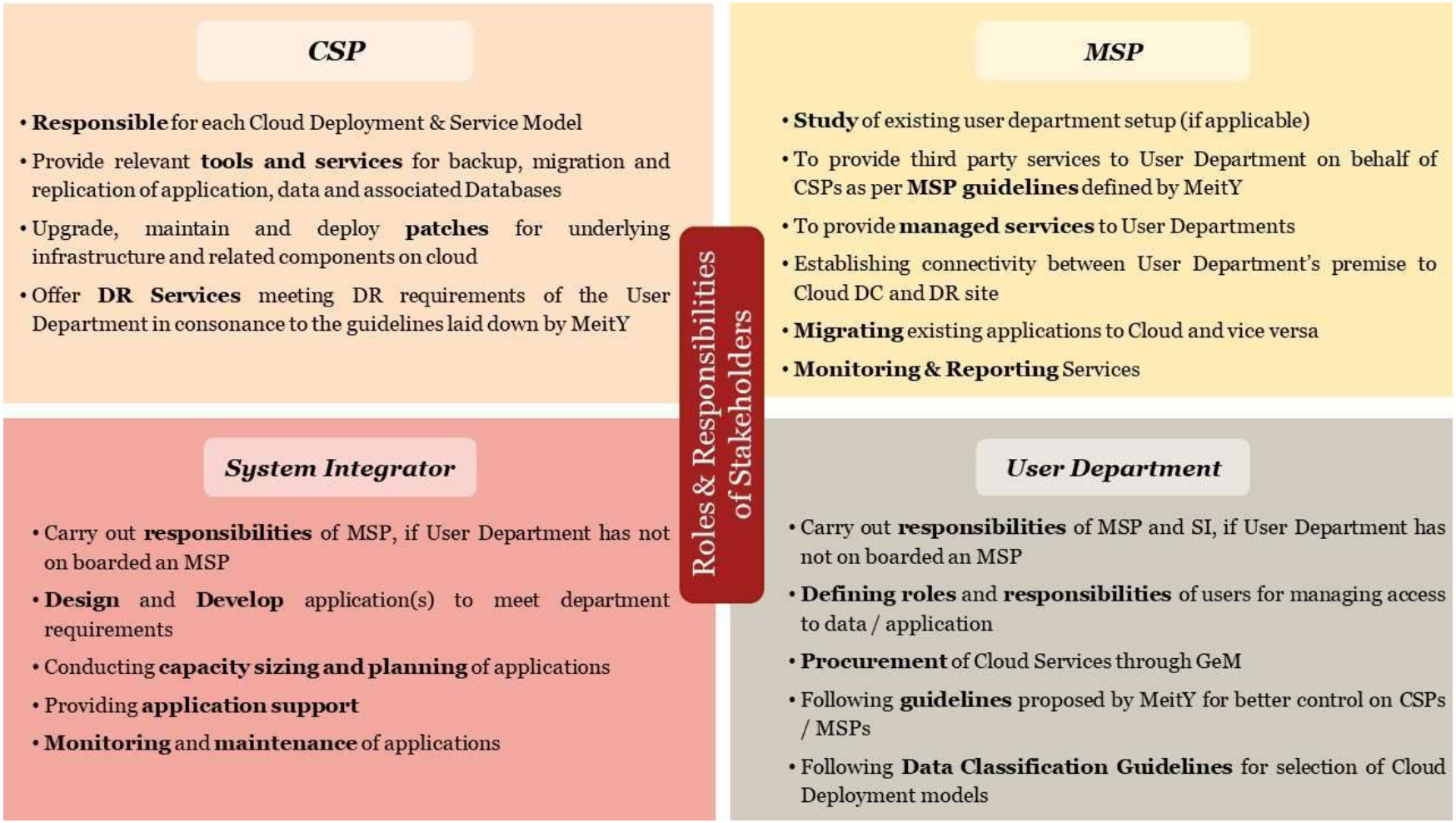


Figure 6: Roles & Responsibilities of Stakeholders

5.3.1 Responsibilities of Cloud Service Providers

This section elaborates the minimum responsibilities of CSP whose services have been empaneled with MeitY and are registered on GeM (Government e-Marketplace) to offer the services.

Below is the non-exhaustive list of responsibilities that a CSP shall be responsible for, however the Government Department may add scope as per their requirement at the time of selection of any CSP and their Services.

1. **Responsibilities for each Cloud Deployment Model:** Set up the required infrastructure and deliver services as per the requirements specified in the CSPs empanelment RFP for the Cloud Deployment Models i.e. Public Cloud, Virtual Private Cloud and Government Community Cloud. The indicative list of Responsibilities of CSP for each Cloud Deployment Model is listed as below: -
    a. Provision and offer services in accordance with the Cloud Deployment Model
    b. Provisioning of managed Virtual Machines
    c. Provide interoperability support with regards to available APIs, data portability etc.
    d. Provide self-service tools to the Government Departments that can be used to manage their Cloud infrastructure environments
2. **Responsibilities of CSP for Infrastructure as a Service (IaaS):** The CSP shall be responsible for managing and controlling the underlying Cloud infrastructure including compute, operating systems, storage, network, security, etc. The indicative list of responsibilities of CSP for IaaS Cloud Service Model is as follows: -
    a. Provide Compute, Storage, hypervisors, network interfaces and other fundamental compute resources
    b. Provide redundancy and high availability for the IT infrastructure (IT Hardware – compute, network, storage, security) to meet the guidelines and SLA terms as laid down by MeitY.
    c. Provide auto-scalable, redundant and dynamic computing capabilities for virtual machines created as a part of the provisioned infrastructure.
3. **Responsibilities of CSP for Platform as a Service (PaaS):** The CSP shall be responsible 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 Government Department. The indicative list of responsibilities of CSP for PaaS Cloud Service Model is as follows: -
    a. To meet all indicative list of responsibilities as mentioned for IaaS

b. Provide platform for development, deployment, operations, and support of applications built by the Government Department on platform services procured by them.
c. To provide the platform with required licenses backed by ongoing support from OEM

4. **Responsibilities of CSP for Software as a Service (SaaS):** The CSP shall be responsible to offer the Government Department with applications running as a service, along with its security, network, storage requirements, upgradation and patching of application, its maintenance and performance, on selection of SaaS, as a Cloud Service Model by the Government Department. The indicative list of responsibilities of CSP for SaaS Cloud Service Model is listed as below: -

    a. To meet all indicative list of responsibilities as mentioned for IaaS and PaaS
    b. To ensure that any service offered from SaaS are monitored, controlled, and administered using web-based tool with visibility to the Government Department.
    c. 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 Government Department's performance requirements.
    d. Ensure zero data leakages (backdoors into the offered SaaS services)

5. **Network Port Connectivity:** Ensure network port connectivity for links between the Government Department location(s)/Infrastructure and other Cloud environments (DC/DR)

6. **Tools:** Provide relevant tools and services for backup, migration and replication of data, application and associated Databases

7. **Security:** Ensure appropriate physical and logical security controls for Cloud deployment and service models as envisaged by MeitY

8. **Patch Management:** Upgrade, maintain and deploy patches for underlying infrastructure and related components on cloud

9. **Disaster Recovery:** Offer DR Services meeting DR requirements of the Government Department in consonance to the guidelines laid down by MeitY

10. **Cloud Access Logs:** Provide authorized access to logs of all user activity within an account and the recorded information including API details, etc.

11. **Data Privacy:** To ensure data privacy guidelines as defined by MeitY or Government Department or Govt. of India are met by the CSP/MSP as applicable during the migration and other Cloud related activities

12. **Exit Management:** To provide support to the Government Department in case of Cloud to Cloud migration, for transferring data & applications, its associated databases, at the time of exit management and in line with the guidelines defined by MeitY.
13. **Compliances:** 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.
14. **Audit Support:** Provide support during Audit by STQC / MeitY empaneled agency or any agency appointed by the Government Department.

5.3.2 Responsibilities of Managed Service Providers

This section refers to the "Guidelines for Managed Service Providers" published by MeitY. MSPs are authorized partners of Cloud Service Providers whose services are empaneled by MeitY and registered on GeM (Government e-Marketplace) for offering it to the Government Departments.

5.3.3 Responsibilities of System Integrator / Implementation Agency

This section lists down the indicative responsibilities of System Integrator whose services are being procured by the Government Departments. In case the Government Department has on-boarded the SI to also carry out the scope of MSP, the responsibilities as mentioned in Guidelines for Managed Service Providers as referred above, published by MeitY shall be applicable to be performed by the SI.

The responsibilities specific to a System Integrator include but not limited to are specified as below: -

1. **Requirement Gathering:** Gathering requirements, including business, system and functional, from the Government Departments
2. **Requirement Mapping:** Map key functional and non-**functional** requirements with the optimal solutions offered by the CSP
3. **Design & Develop:** Design and Develop **application**(s) / software(s) to meet department needs / requirements
4. **Capacity Sizing:** Conduct Capacity Sizing and **planning** for applications
5. **Application Lifecycle:** Build, Test and Deploy applications for the Government Department on the CSP platform
6. **Integration Services:** Provide integrations services for applications as per the requirement
7. **Test Plans:** Executing Test plans to test **application** functionality
8. **Change Requests:** Provide services specific to change requests raised by the Government Department

9. **Patch Management:** Upgradation and **patching** of application, it's database and maintenance
10. **Support Services:** Providing application **support** in case of any technical error or glitch
11. **Any other requirement** as specified by the **Government** Department

5.3.4 Responsibilities of Government Department

This section elaborates the responsibilities of a Government Department, who intends to procure Cloud Services through GeM or RFP and looks forward to migrating to Cloud.

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

The overall roles and responsibilities of a Government Department includes but not limited to:

(i) **Roles & Responsibilities:** Defining the roles and responsibilities of users for managing access to data / application

(ii) **Security:** Ensuring the security of the endpoints that are used to access Cloud services (as applicable)

(iii) **BCP & DR Policy:** Draft and Prepare BCP and Disaster Recovery policy in tandem with CSP

(iv) **Backup & Retention Policy:** Draft and Prepare Backup and Retention policy in tandem with CSP

(v) **Migration:** Decide on Data / Applications to be migrated

(vi) **Approvals:** Providing approvals to CSP/MSP/SI for all types of request(s) submitted

(vii) **Review and Validate:** Review and validate security configurations created by CSP / MSP / SI

(viii) **Performance Monitoring:** Review the performance monitoring and resource utilization reports submitted by CSP/MSP/SI and initiate necessary action, as required

(ix) **Billing:** Verify billing and metering resource usage details for procured Cloud Services

(x) **Compliances:** Specify additional project specific compliances, certifications, requirements, guidelines, etc., while procuring or availing Cloud Services

(xi) **Content Management:** The Government Department shall be responsible to for the development, operation, maintenance and use of their content and ensure that the content stored by the Government Department or its users does not violate any of the policies or any applicable law.

5.4 Evaluation Framework for CSP

This section of the document highlights the key considerations and suggestive evaluation framework, which a Government Department should deliberate during evaluation and selection of Cloud Service Providers.

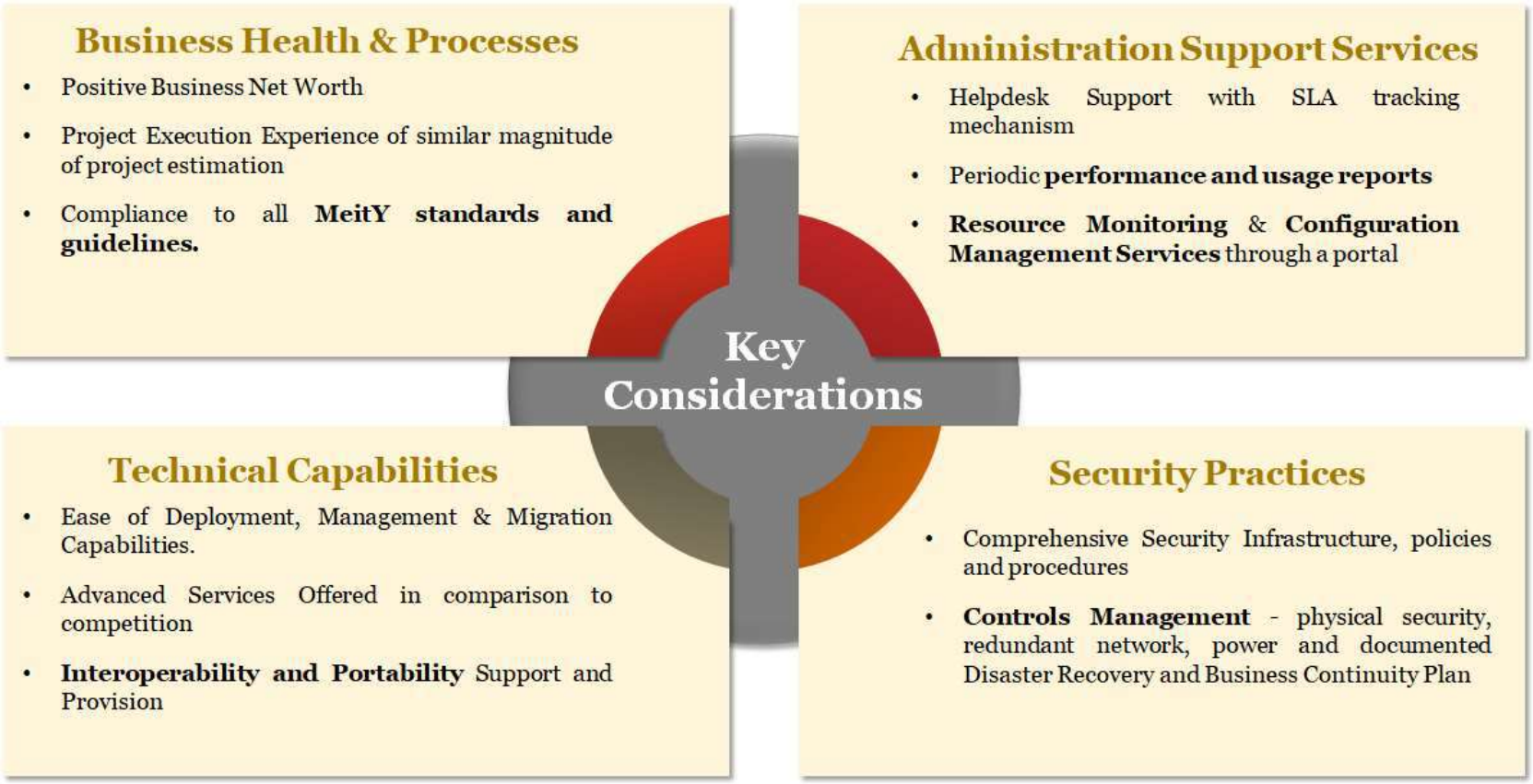


Figure 7: Considerations for Evaluation of CSP

The following info-graphic details the suggestive evaluation framework for selection of CSP. The Government Department may use / amend the framework as per their requirements

Evaluation Framework for Selection of CSPs:

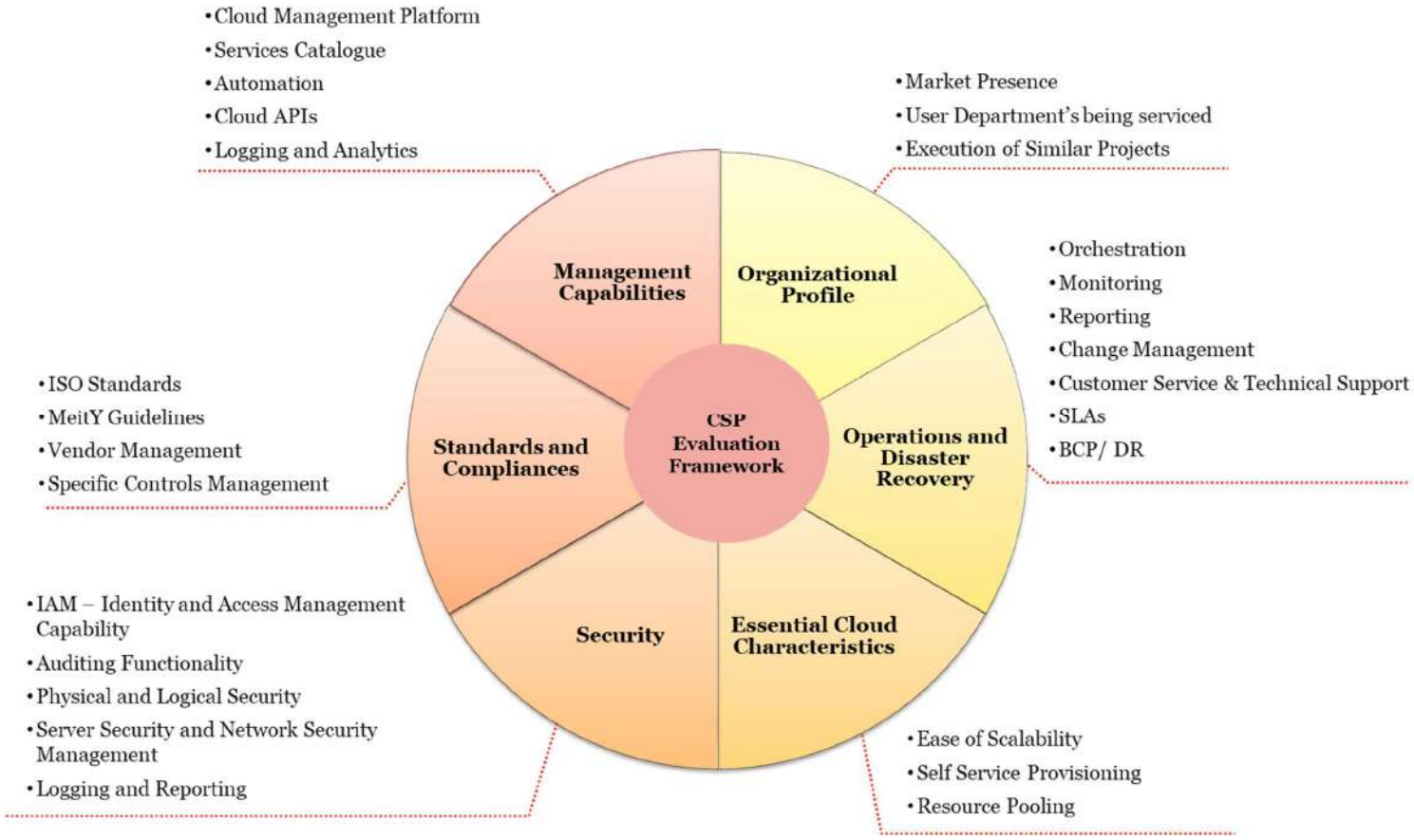


Figure 8: CSP Evaluation Framework

5.5 Integration with Internal & External IT Systems of the Government Department

5.5.1 Approach and Methodology towards Integrating Cloud Services

Government Department integrating internal IT system or external IT systems hosted in various Data Centers or Cloud Service Provider platforms with Cloud Services procured by Department has started picking pace as it brings new processing capabilities without having to introduce major changes in the existing system. To benefit from Cloud adoption and reduce challenges, integrating internal or external IT system with cloud services is a win-win solution that takes advantages of cloud services with lower investment, especially for the Government Department that have been running multiple IT systems on-premises for years.

Integration involves creating cloud-to-cloud integration, cloud-to-on-premises integration or a combination of both. Integrations can address different business components, including data and applications. The various types of Integration with respect to IT systems is as follows:

- **Cloud-to-Cloud Integration** – Integration between two or more cloud platforms offered by MeitY empaneled CSPs.
- **Cloud-to-On-premise/Local Integration** – Integration between cloud platform of a MeitY empaneled CSP and on-premises environments of the Government Department/ NIC/ State Data Center or any mix of the two.

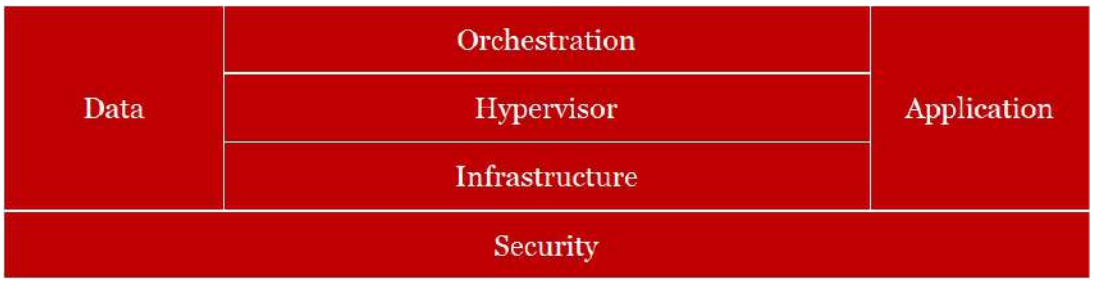


Figure 9: Components in a Cloud Deployment

The above figure depicts the major components which constitute a cloud deployment. Infrastructure is the base line for establishing a cloud platform over which resides the hypervisor for virtualization. The orchestration layer is responsible for management of the cloud deployment and Security encompasses the entire deployment.

Direct infrastructure integration is not supported whereas integration through hypervisor, security, data, application and orchestration is possible to achieve.

An application deployed on the cloud platform may integrate with external systems and generate data in the process. Application Integration connects various applications and enables continued functionality and interoperability. In this type of integration, two or more applications can share states, requests, commands and other mechanisms to implement businesses processes. Through application integration, a Department can link

applications to share data and automate broader business practices. API integration is a methodology to achieve application integration

5.5.2 Integration with Cloud Service Models

The integration of Government Department's IT systems with SaaS maybe done with the motivation of achieving immediate business value and productivity enhancement. For PaaS, the objective of integration could be to enhance software development life cycle management and the integration intent for IaaS could be to enable scalability and reliability of hardware resources without changing the existing IT infrastructure.

From the perspective of a Government Department various technical aspects dictate the extent of integration possibilities and have been highlighted as below:

Technical Aspects / Cloud Service Models	Traditional Data Center	Resource Manageability	Service Manageability	License Management	Security Manageability
IaaS	DC IT Infrastructure is Government Department responsibility	Available for Government Department	Available for Government Department	Available for Government Department	Available for Government Department
PaaS	Middleware Management is Government Department responsibility	Not Available for Government Department	Available for Government Department	Not Available for Government Department	Available for Government Department
SaaS	Application for Government Department use only	Not Available for Government Department	Not Available for Government Department	Not Available for Government Department	Available for Government Department

The Cloud Service Models pose an opportunity to allow integration with internal and external IT systems and allow various management options to government departments to facilitate such integrations.

1. **Integration of IaaS:** IaaS can be provided by different cloud service providers as empaneled by MeitY. With the new-age technologies, the integration between On-premise IT systems and IaaS has become quite seamless as the existing IT systems can be upgraded without having to make any changes in software or applications and the storage capability and computation units can be easily expanded.
    a. For any IT system, servers are crucial and at any point of time, the workload of servers may exceed the usually expected required capacity. Clustering technology is essential to allow the workload balancing within different servers provided

through cloud and make full use of the servers. With load balance techniques, the utilization can be optimized.

b. In IT system, all the computing and processing are done on servers instead of on clients, by clustering and load balance, some server or computing resource cloud be automatically allocated to IT system dynamically.

c. Data synchronization should be considered when integrating IaaS and IT. For implementing IaaS integration, an optimal network is essential.

d. Integration at IaaS level extends computation capacity. Integration of IaaS and traditional IT can be achieved by following two ways:

   i. Virtualization technologies: It allows the system administrators to establish multiple virtual servers (Virtual Machines) based on pool of hardware resources, but the virtual servers are not to be bound to physical devices. Full virtualization can be achieved using hypervisor. It interacts directly with the physical server's CPU and disk space. It serves as a platform for operating systems, virtual servers. The hypervisor provides independence and autonomy of each virtual server to other virtual servers running on the same physical machine. Each guest has its own operating system.

   ii. Distributed technologies: They are used to permit data to be stored on different physical devices, but the data can still be used as one entity.

2. **Integration of PaaS** and **SaaS:** Applications are rarely developed and run on a PaaS platform completely standalone. Usually these applications should integrate with the existing IT systems like applications, services, data, etc. Few of them are likely to be present in an existing organizational environment outside the cloud system. There are two approaches for mapping the data between PaaS/ SaaS system and Government Department IT systems. The connection can be built on batch-style basis or the organizational data can be revised whenever the PaaS/ SaaS application carries out a transaction which modifies the Department data. The approaches are mentioned below:

   a. API Management

      i. An API Management module can be installed to expose a controlled set of capabilities of single or multiple enterprise systems as an API which might be called by PaaS/ SaaS application.

      ii. The API Management module will also manage the security of the API and limiting API access to specific PaaS/ SaaS applications.

   b. Secure Connector

      i. A component which can manage application-to-application connectivity and provide database-to-database connections.

      ii. The database connectivity approach is advantageous where direct access from PaaS application to enterprise data is advisable.

      iii. When the amount of transactions from PaaS application are large in volume for the department's IT system or when the data goes through

a difficult transformation to become usable by PaaS application this approach is more usable.

iv. The database-to-database connector provides the competence to transform data between enterprise data systems and data services in PaaS environment, with PaaS services built to handle the interactions with PaaS application.

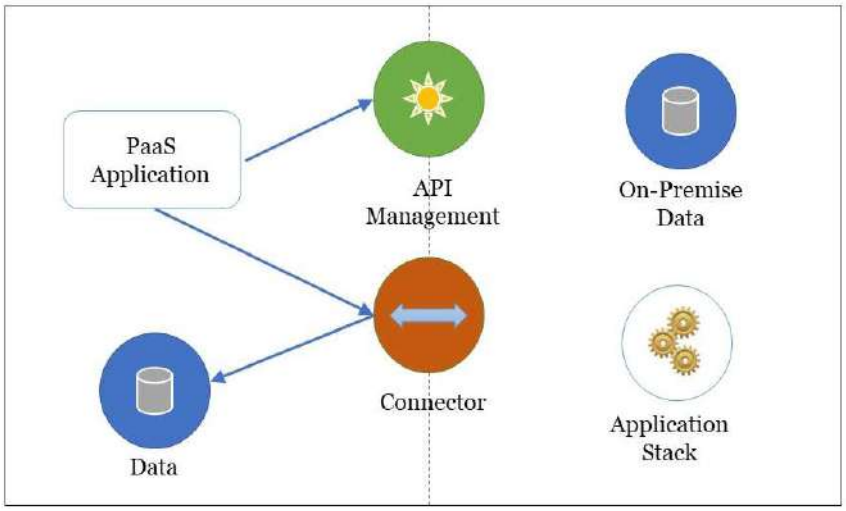


Figure 10: Integrating PaaS applications with existing IT systems.

5.5.3 Use Cases for Integration

The various use cases for IT integrations for Government Departments are described as below:

1. **On-premise DC to Cloud DC site (Hybrid Cloud)**: A hybrid cloud platform is one of the ways to integrate distributed setups. Government Departments experience a compelling feel by connecting anything, anyone, and anywhere from core on-premises systems all the way to edge IoT devices. Hybrid integration enables Government Departments to run their data exchange/ Applications and technology using a blend of two distinct deployments – cloud and on-premise. A Hybrid cloud integration would enable Government Departments to:

    a. Integrate on-premise systems and applications with SaaS applications and cloud services

    b. Leverage the best available technologies that give the Department the platform to achieve its goals

    c. Scaling in case of increasing data requirements.

    The managed services route in a hybrid cloud integration means the Department can free internal resources from managing applications, save on hardware investment and maintenance costs, and reduce resources spent managing complex integrations and focus on core initiatives that will progress towards achieving Department goals.

2. **On-premise DC to Disaster Recovery (DR) Site on Cloud**: Setting up replication between On-premise data center and the cloud platform of a MeitY empaneled Cloud Service Provider. The Government Department or the Managed Service Provider (MSP) can setup the cloud-based platform as the DR site for the primary hosted on-premise/ NIC Data Center/ SDC. The replication is configured between the sites (Application, Database or Storage Level) by either the Government Department or the MSP. In case of a disaster depending the RPO and RTO, the DR site on cloud can act as a primary site running the application workload of the Government Department.
3. **DC on Cloud to DR Site on Cloud**: Both sites of the Government Department are hosted on the Cloud Platform of the same Cloud Service Provider or different Cloud Service Provider. Native Cloud tools may be employed to configure the DR site for the Primary on Cloud including replication.

A few indicative guidelines for integrating Cloud Services with Internal IT Systems and External IT Systems are as follows:

S No.	Indicative Guidelines
1	The data in transit between On-premise and Cloud setup and between different Cloud Platforms is suggested to be encrypted to ensure data protection.
2	Ensuring Advanced API Security at Application Level is suggested when connecting with PaaS and SaaS models.
3	Avoiding Data De-duplication between various environments when integration of platforms is undertaken is suggestively a good practice.
4	User Access Control through Active Directory and other Identity and Access Management software is suggested to be undertaken by the SI of the Government Department or the Government Department itself.
5	Ensuring necessary connectivity (VPN, P2P, MPLS) to both sites (On-premise to Cloud or Cloud to Cloud) between which integration is to be facilitated.
6	Ensuring service level integrations where Service Level Agreements for on-premise and cloud shall be different, and all such SLAs need to be well integrated for smooth performance.
7	Documenting regular changes being made to PaaS and SaaS is a suggestive practice which may have direct impact on integration with various platforms.
8	Important to have Application Vendors design Business Logic flows between source and target systems so that data integration is quicker and seamless with less opportunities of inconsistency.
9	Perform central management and monitoring of the workloads spread across cloud platforms and other data centers

The Government Departments may include additional guidelines to facilitate integration of Cloud Services with Internal and External IT Systems of the Department.

5.6 Migration Planning

This section of the document helps you design a plan when migrating to Cloud. It discusses considerations and indicative steps, and a template for migrating your existing workload to the Cloud platform. This section shall further help a Government Department to use the different templates as attached below.

The indicative migration template as given in Annexure 3, elaborates the phase vise approach of the various tasks that need to be carried out during migration, estimated no. of days and downtime that a Government Department needs to evaluate along with CSP / MSP, when planning for migration.

The indicative draft template for planning of migration of Government Department's existing workloads to Cloud is attached for ready use by Government Departments. The attached file covers, indicative Cloud Migration template for Current environment, high-level migration phase plan, and application migration checklist.

Cloud Migration Template

S. No	Application Name	Current Application Platform	Current Database (with version)	Business Critical (High/Medium/Low)	Existing Server Name & Configuration			Latest Supported Platform version (Windows 2016 Server, .Net4+, IIS7+)	Latest Supported Datatbase Version, 2016 & above	Proposed Server Configuration (if migrating to cloud), Processor, RAM, HDD, IOPS				Migration Priority (High/Medium/Low)	Application Vendor	Remarks (if any)
					Server Name	Existing Cores	Existing RAM			vCPU (V Cores)	RAM	HDD	IOPS			

Application Migration Checklist

Current Application Status							
Application Name	Application Size	Database Name	Database Size	Application Full Backup Size	Database Backup Size	Application Backup Date and Time	Database Backup Date and Time

On Cloud													
Down Time Required (Date & Time Window)	Down Time Approval Status (Yes / No)	Notification to all users & Internal teams (Yes/No), with time stamp	VM Name	File Path	DB Server Name (VM)	App. Migration Start Date / Time	App. Migration Completion Date / Time	DB Migration Start Date / Time	DB Migration Completion Date / Time	Testing (Yes/No)	Tested By (Vendor)	Verified by (User Department)	Go-Live Date and Time

6. *Stage 3: Build*

Once the capacity sizing and selection of suitable Cloud Models has been completed, the Government Departments should now focus their attention towards the build stage. The section below outlines the procurement guidelines along with guidelines for developing application on cloud to assist Government Departments in this process of Cloud Adoption & Enablement.

6.1 Procurement Guidelines

This section refers to the "Procurement Guidelines" published by MeitY, refer https://meity.gov.in/writereaddata/files/Guidelines_Procurement_Cloud%20Services_v2.2.pdf. The said guidelines may be used by the Government Department for procuring Cloud Services through GeM or RFP and for demarcation of roles of different stakeholders in the process.

6.2 Guidelines for Developing Application on Cloud

6.2.1 Developing Application Architecture in Cloud

Cloud applications are best deployed as a collection of cloud services, or APIs. At its essence, it is a service based or service-oriented architecture. While developing an application architecture for the cloud, following steps should be noted and if applicable adhered to:

1. **Loose Coupling of service:** This is a fundamental concept of Service Oriented Computing. It ensures that applications components are treated individually, and dependencies are reduced. It further ensures that addition, removal, failure or update of one component has a minimum impact on other components. Thus, it is always recommended to develop components separately and defining their integration/ interaction mechanism in a separate component
2. **Service Granularity:** Each service operation should ideally perform single transaction to simplify error detection, error recovery, and simplify the overall design. Each service operation should map to a single business function, although if a single operation can provide multiple functions without adding design complexity or increasing message sizes, it can genetically reduce implementation and usage costs
3. **Decouple the data:** Since private and public clouds are complex distributed systems that work best with application architectures that break out processing and data into separate components. By decoupling, the data can be stored and processed on any public or private cloud instance. In such cases latency may occur, so it is recommended to use caching systems. These provide additional database performance by locally storing commonly accessed data, thereby reducing all database read requests back to the physical database.

   Note: For systems which are constantly reading new data don't benefit much from caching systems.
4. **Intercommunication between application components:** Application components that communicate with each other continuously may lower the performance of the

overall application. In order to improve the performance combining the communications into a single stream of data, rather than constantly sending messages is the best practice.

5. **Model and design for performance and scaling:** Firstly, a test case should be built that represents how an application behaves under an increased load. While the traffic increases, the number of web server and associated database instances may have to be increased to handle any additional load. This can help to understand the process to scale the application by automatically increasing resource on the instances or load balancing. In some cases, Cloud service providers offer auto-scaling capabilities, where provisioning occurs automatically. In this manner, it becomes easier to understand the application's workload profile and defining the path to scaling the application.
6. **Security within applications:** Developing solution architectures that focus on mature Identity and Access Management capabilities can reduce security costs for Government Departments.

   Note: The Government Department may also refer to the Productization guidelines as defined by MeitY, available at https://meity.gov.in/writereaddata/files/Application_Development_Re-Engineering_Guidelines_0.pdf and reproduced below in Annexure 4

6.2.2 Standards to be adopted while Designing Applications

There are a number of standards available for software engineering lifecycles which ensure quality product development and incorporate scope of continuous improvements. The standards are to be followed as per the Government of India issued policies and guidelines promulgated from time to time.

The proposed solutions should be adaptable to the following as good software engineering practices:

1. **Domain / Sector specific Meta Data Standards:** Each sector or domain has its unique challenges in standardization of Meta-Data. It is important that any solution being developed to provide services in the domain or sector adhering to the Meta-Data standards for that particular sector or domain. This would ensure seamless integration between solutions developed for domain or sector. The GOI has also come out with Meta data standards which can be seen at www.egovstandards.gov.in
2. **Software Engineering Standards:** It is important that software engineering standards are adopted during the initial stages of the development lifecycle to ensure that the developed solution is able to meet quality certifications and security testing. Recommended testing requirements will be provided by STQC / empaneled agencies.
3. **Usage of Open Standards technologies:** As part of software engineering, it is important to use technologies developed in open standards. As part of the overall software development lifecycle, a minimum customization and maximum

configuration approach should be adopted wherein there should not be any hard-coding from the aspect of the development.

6.2.3 Documentation and Release Management

It is important for applications to adhere to quality certification processes to ensure that solutions being given for replications to other stakeholders, meets minimum quality benchmarks. To ensure a quality product it would be required that the solution:

1. Should qualify defined functional testing through STQC
2. Should qualify defined performance testing through STQC
3. Should qualify defined security testing
4. Should have well documented development & testing process artifacts
5. Business Requirements Document (BRD)
6. Functional Requirement Specifications (FRS)
7. Software Requirement Specifications (SRS)
8. Software Design Documents (including HLD, LLD etc.)
9. Requirements Traceability Matrices (RTM)
10. Test Plan, Test Cases & Test Reports
11. Code Review Reports
12. Database Review Reports
13. Project Implementation Plan User Manual
14. Deployment Guide

6.2.4 Solution Sizing & Scalability

Although an initial estimation of the hardware specifications (quantity and model / version) would be required to size the solution based on system interaction, to increase capacities the solution should adaptable to scaling. The following should be kept in perspective:

1. **Able to scale up to meet increasing load:** Solution Design should be able to handle increasing number of first-time users, transactions, data sharing processes etc.
2. **Able to demonstrate stress levels exerted:** Solution Design should be able to handle increasing number of concurrent users, concurrent transactions, synchronous data sharing with other systems etc.
3. **Able to perform on throttled bandwidth environments:** Solution Design should be able to perform to the agreed service levels regardless of the bandwidth availability.
4. **Should have low technical & infrastructure resource consumption:** Solution Design should optimally use technical resources such as memory, processor (CPU), storage etc. In addition should optimally use of Cloud resources on available bandwidths.
5. **Should be interoperable to newer technology upgrades:** The Solution Design should be able to harness the advantages of legacy technology (servers, software, devices etc.) while be able to upgrade to newer systems. This would enable low cost – optimal utilization of resources.

7. Stage 4: Implement

Post the completion of Build Stage wherein the procurement has been completed and application has been prepared for migration begins the stage of Implementation. This stage involves preparing the cloud environment on the CSP platform, installing and configuring the applications, strengthening the production environment, executing mock migration, final migration and Go-Live to production cloud. The goal is to ensure all activities are performed in a sequential manner, while minimizing downtime and disruption to users.

7.1 Cloud Platform based Service Development

Government Departments may use Cloud platforms for a range of hosted services for compute, storage, and application development. The Departments and their IT administrators along with the SIs can access the Cloud Platform services over public Internet or through dedicated network connection like VPN.

Ministry of Electronics & Information Technology (MeitY) has empaneled multiple Cloud Services for three different Cloud service models:

- Infrastructure as a Service (IaaS)
- Platform as a Service (PaaS)
- Software as a Service (SaaS)

The Government Departments can select any of the empaneled Cloud Service model as per their requirement. Each of the Cloud Service model have their own benefits, as well as variances and it is necessary for the Government Departments to understand the differences among IaaS, PaaS & SaaS to know how to best choose one of them, as per their requirement.

IaaS and PaaS models allow the Government Departments to develop services over the platform, however, in case of SaaS, the Government Departments get ready to configure and consume software and licensing from the CSPs. The delivery model of PaaS is similar to SaaS, except instead of delivering the software over the internet, PaaS provides a platform for software development and rollout. This platform is delivered via the web, giving SI/application developers of the Government Departments, the freedom to concentrate on building the software without being concerned about the operating systems, software updates, storage, or infrastructure which shall be CSP/MSP responsibility. The below table illustrates the responsibilities of the Government Department and the CSP with respect to service development in IaaS and PaaS:

Cloud Service Models	Development Environment License	Tools	Lifecycle Management of Code	Infrastructure
IaaS	Government Department	Government Department	Government Department	CSP
PaaS	CSP	CSP	Government Department	CSP

In case of PaaS model, the Government Department has two options for buying the licenses and tools from the CSPs:

- Use License as a Service as per the Industry standards
- Use proprietary tools made available by CSPs from their platform

The Government Department must take care of the below parameters while developing any services over the Cloud platform:

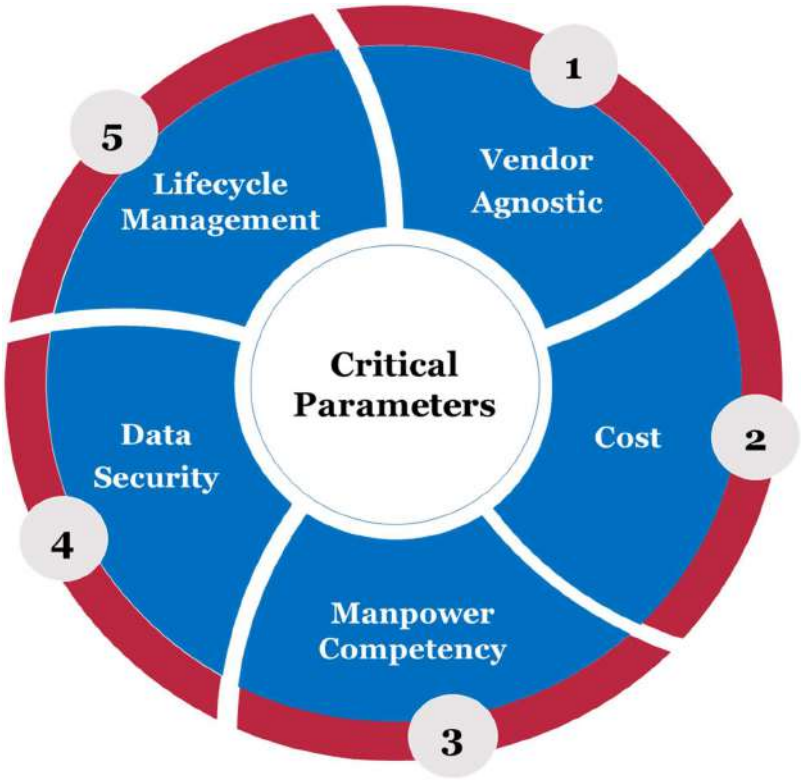


Figure 11: Parameters for Platform based Service Development

- **Vendor Lock In -** The Government Department must be aware about the vendor lock-in constraint with PaaS. Unlike IaaS, PaaS often requires the use of a specific, proprietary languages, tools and licenses. This can cause an issue if a Government Department wants to migrate to a different PaaS provider. The Government Department must research PaaS providers thoroughly before developing applications. If the vendor has not provisioned convenient migration policies, switching to alternative PaaS provider could be a challenging task.
- **Cost –** PaaS leverages a better cost benefit to the Government Departments as compared to deploying an equivalent platform on premise where the Government Department in case of PaaS can procure services on need basis and exit without any OEM lock in and associated licenses and support cost.
- **Manpower Competency** – The CSPs offering their platforms for service development are often based on a single, proprietary languages, tools and licenses, hence, this may create

a challenge for the Government Departments who have not on-boarded an MSP or SI who can leverage their expertise according to the Government Department would need to hire a team of resources having similar expertise.

- **Data Security -** Government Departments can run their own applications and services using PaaS solutions, but in parallel should keep a check on the security controls, to ensure the security of their data at rest and data in transit. The Departments, while developing the services must be fully aware of the security features being offered by various CSPs and make use of the same while consuming PaaS.
- **Lifecycle Management –** Lifecycle Management of Code means the specification, design, development and testing of a service/application. It is important that the lifecycle of the source code is maintained by the Government Department (or its on-boarded SI) and covers the entire cycle from idea conception to development, testing, deployment, support and ultimately retirement of systems. An example of management could be DevOps. DevOps is the combination of cultural philosophies, practices, and tools that increases the ability to deliver applications and services at high velocity: evolving and improving products at a faster pace than using traditional software development and infrastructure management processes. This speed enables Government Departments to roll out better services to citizens and other Departments.

7.1.1 Limitations and Concerns of Service Development on Cloud

- **Integration:** The Government Department must consider their legacy applications and evaluate their readiness and maturity to work in a IaaS and PaaS environment. The Government Departments should consider these platforms only for applications that are mature enough to utilize the benefits of this model. Particularly when not every component of a legacy IT system is built for the cloud, integration with existing services and infrastructure may pose a challenge.
- **Customization of legacy systems:** PaaS may not be a plug-and-play solution for existing legacy applications and services of the Government Department. Instead, Government Departments will be required to do several customizations and configuration changes for legacy systems to benefit from the PaaS offering. The resulting customization may result in a complex IT system.
- **Version issues:** The Government Departments must be aware that the specific framework versions may not be available or perform optimally with the PaaS offering.
- **Operational Limitations:** Customized cloud operations with management automation workflows may not apply to PaaS solutions, as the platform tends to limit operational capabilities for Government Department. Although this is intended to reduce the operational burden on end users, the loss of operational control may affect how PaaS solutions are managed, provisioned, and operated. The same may not be applicable in case of an IaaS offering where the Government Department is responsible for provisioning platform suitable for service development on the procured infrastructure.

7.2 Migration Roadmap

This section covers the migration road map for the Government Departments who intend to migrate their application workload to Cloud, including various phases for migrating an application to Cloud. The below figure highlights the different categories in which a Government Department may position its application in accordance with the time required to migrate the application to Cloud.

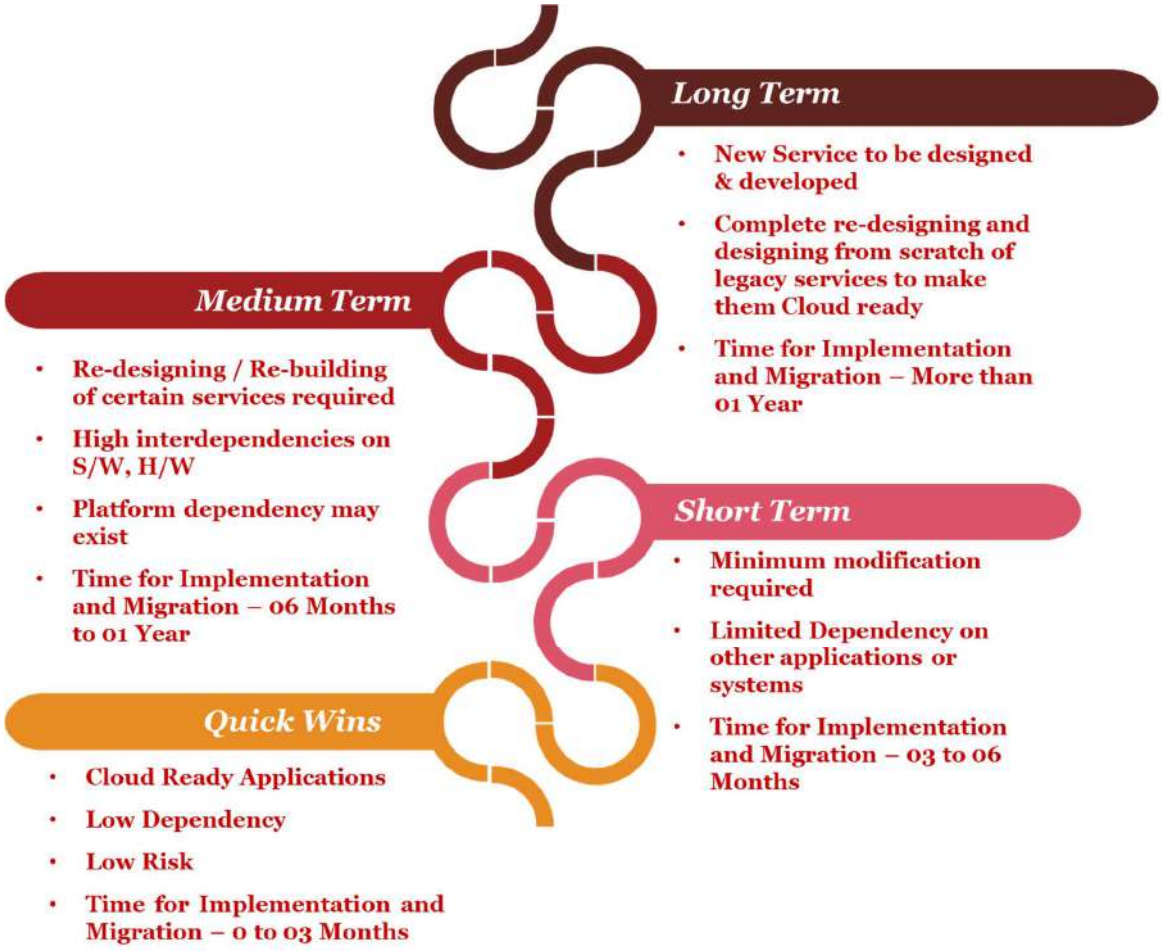


Figure 12: Migration Roadmap

The phases as highlighted below are designed to give Government Departments and approach towards successfully migrating their workloads to Cloud in a streamlined and an accelerated manner. The various phases of migrating an application to Cloud are supplemented with indicative outcomes and deliverables which may be project specific and Government Departments may amend the same as per their understandings & requirements.

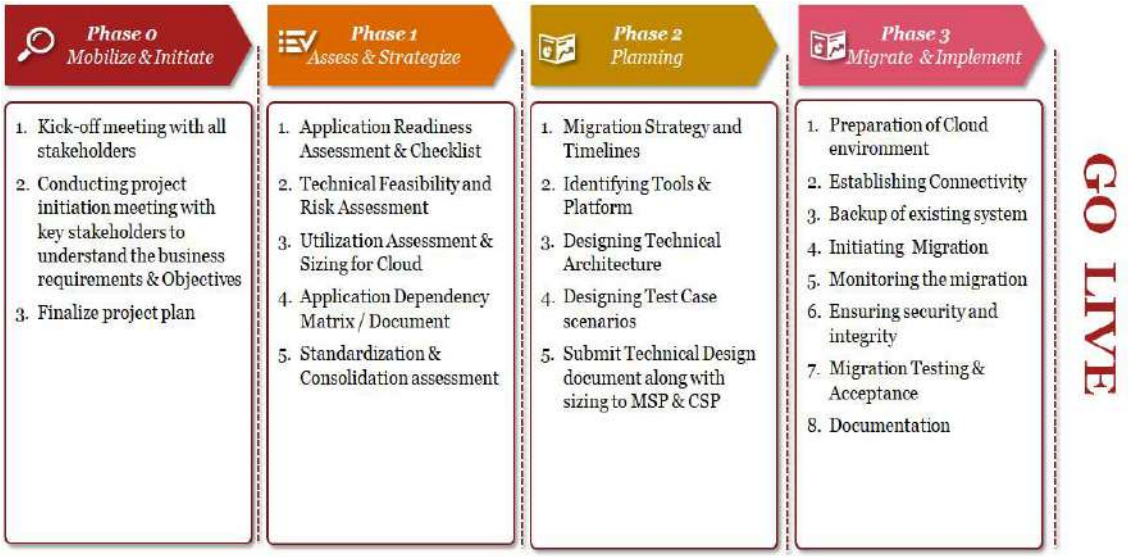


Figure 13: Migration Roadmap Phases

The above phases of Application Migration Roadmap are detailed as follows:

7.2.1 Phase 0: Mobilize and Initiate

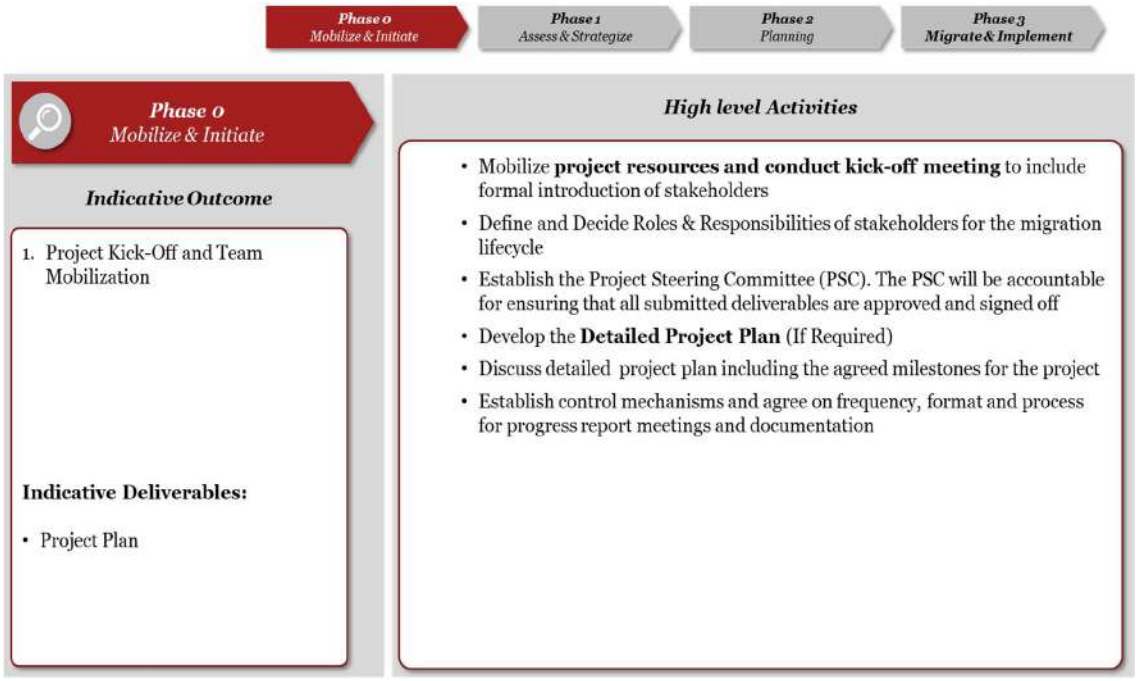


Figure 14: Phase 0 - Mobilize & Initiate

7.2.1 Phase 1: Assess & Strategize

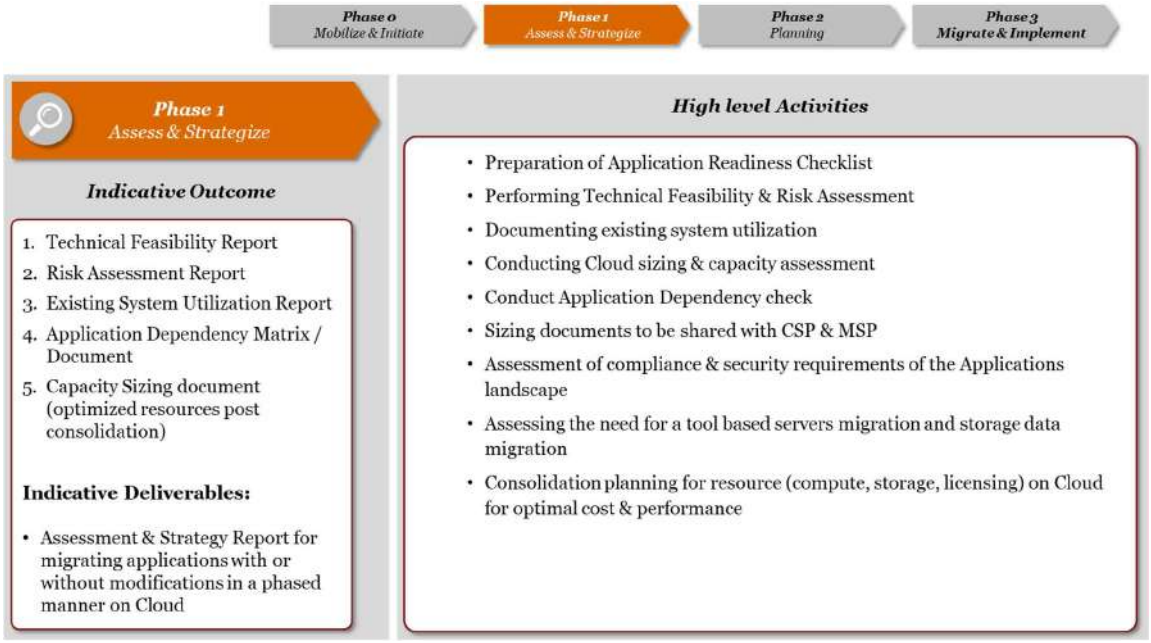


Figure 15: Phase 1 - Assess & Strategize

7.2.1 Phase 2: Planning

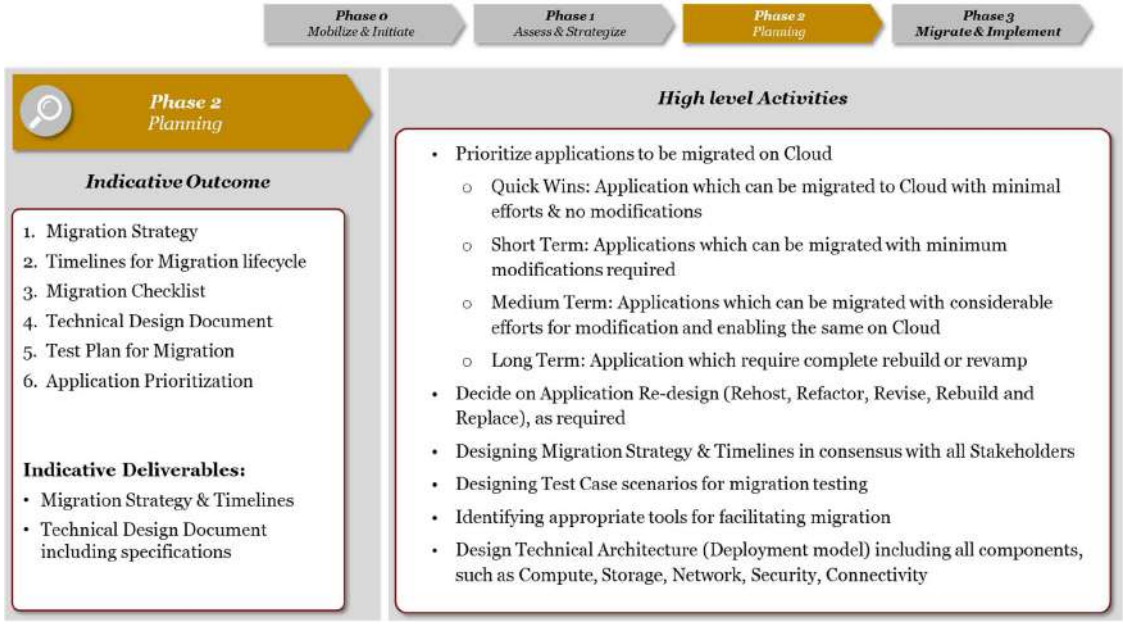


Figure 16: Phase 2 – Planning

7.2.1 Phase 3: Migrate & Implement

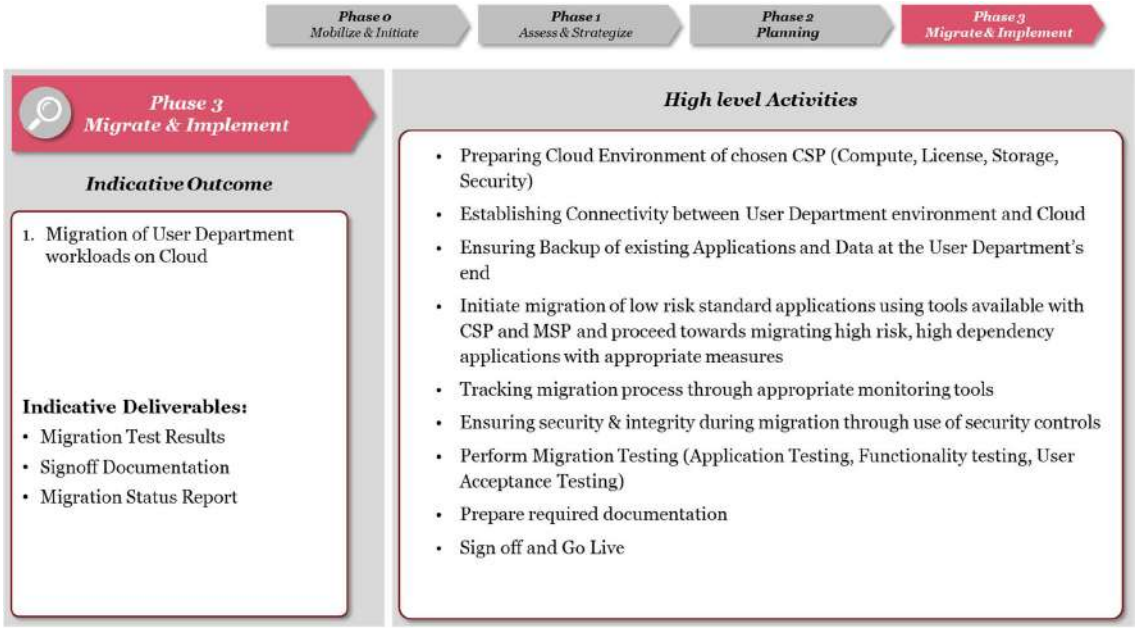


Figure 17: Phase 3 - Migrate & Implement

Re-architecting applications

While the Government Departments move towards cloud adoption it is pertinent for them to evaluate the migration roadmap to choose a suitable Cloud Services Platform that would be in-line with their business needs and further assist in transforming the Government Department as a whole. While certain applications would be cloud ready in nature possessing minimum dependency on other applications along with a low risk profile while other applications would be legacy in nature and completely redesigning and coding them would be the appropriate methodology to upgrade and deploy on cloud.

Determining the right migration strategy for an application depends on its level of cloud alignment, cloud readiness, potential benefits achieved from migrating, and risks. The different approaches to move to cloud are as follows:

- **REHOST on Infrastructure as a Service (IaaS):** This approach involves the re-hosting of the application from the existing infrastructure to the cloud infrastructure without making any significant changes to application code-base or the application configuration files. The application Operating System / Hypervisor along with the Hardware is managed by the CSP.
- **REFACTOR for Platform as a Service (PaaS):** This approach involves the refactoring of the application to use the platform provided by the CSP to migrate the application. In this method the programming languages, development frameworks, containers, operating system / hypervisor and the hardware are all managed by the CSP/ MSP. In addition, application data is kept the same or transformed upon migration, application source code is updated, application configurations are extended to service the

Government Department and programming languages and development frameworks are either kept as the same or new ones provided by the platform are used.

- **REVISE for IaaS or PaaS:** This approach involves the migration of the application requiring rebuilding the application utilizing either the infrastructure components of the cloud or utilizing the platform components of the cloud. In this approach like the Refactor approach, programming languages, development frameworks, containers, operating system / hypervisor and the hardware are managed by the CSP/ MSP; while the application data, source code and application configuration is managed by the SI or the Government Department. In addition, the application data is kept the same or transformed, the source code is updated, new application configurations are required, same or new programming languages, development frameworks and containers are used for revising applications.
- **REBUILD on PaaS:** This approach involves the redevelopment of the application to suite cloud-based deployment. Similar to the revise approach, in this approach also the programming languages development frameworks, containers, operating system / hypervisor and the hardware are managed by the CSP/ MSP; while the application data, source code and application configuration is managed by the SI or the Government Department. In addition, the application data is transformed from the existing infrastructure to the new environment, the source code and application configurations are written / configured anew. The existing or new programming languages and development frameworks from the cloud platform are used.
- **REPLACE with Software as a Service (SaaS):** The last approach for migration of the applications to cloud involves replacing the existing application with a new application, which is completely managed by the CSP/MSP, and is available to the Government Department on the Software as a Service (SaaS) Model. In this approach the application data from the existing application is transformed to the new application; while all other aspects such as source code, application configuration, programming languages, development frameworks, containers, operating system / hypervisors and hardware are managed by the CSP/MSP.

8. Stage 5: Management & Monitoring

This section of the document has been designed to enable the Government Department in adopting a monitoring approach during and post migration with an objective to track progress of ongoing migration of different workloads of the Government Department and performance post migration indicating any operational, performance issues such as data discrepancy. Further, it is also important to manage different application vendors and service providers for achieving a seamless migration of Government Department to Cloud. A successful migration is subject to the Government Department achieving performance improvements and the newly migrated system enabling the Government Department to achieve their business objectives.

Below are the suggestive guidelines, which a Government Department may use and adopt during the management and monitoring phase. The Government Department may add any additional guidelines relevant to their needs and specific requirements.

1. The Government Department post migration should monitor system performance and utilization using Enterprise Monitoring tools made available by the CSP/ MSP, thus enabling them with system wide visibility and in turn assisting them in optimizing system performance as per need.
2. Scaling up (Increasing) and Scaling down (Decreasing) of cloud resources (Virtual Machines, Compute, Memory, Storage, Bandwidth) may be identified by the Government Department post migration and testing of the system to understand application performance and response on Cloud.
3. The Government Department should analyze application response post migration by employing Application and Database Performance Management tools made available by CSP/ MSP to understand system bottlenecks if any and help Application Vendors/ SI to optimize Application and Database Design if required.
4. Post migration, the Government Department should ensure application workloads migrated to Cloud meet the required benchmarks and controls as specified by the Government Department and guidelines laid down by MeitY and ensure if performance expectations are met before Go-Live In case the Government Department's expectation from Application Response are not met post migration the Application and Infrastructure Architecture may need to be re-done. The Government Department in tandem with the MSP/ CSP to make relevant changes and implement the same on Cloud.
5. The Government Department must perform rigorous Data Integrity Checks at Application and Database Level post restoration during migration as the process of migration (installation and configuration/ restoration of application and database on cloud) may need to be re-done in case of data errors or loss.
6. The Government Department should keep a regular track of the health of Virtual Machine instances, storage, networks being used in the cloud environment for their workloads

7. The Government Department must ensure the Managed Service Provider must provide managed services for various components on the cloud as per the scope of work finalized and the MSP must share relevant reports with the Government Department periodically as outlined in the MeitY guidelines or as per the scope of work signed off between Government Department and the MSP. The Government Department shall ensure that the CSP/ MSP may perform the following tests post migration:
8. Infrastructure testing - various testing procedures including infrastructure (server, storage and network infrastructure) provided on Cloud.
    a. VM testing
    b. Storage/Disk IO testing.
    c. Network throughput and latency testing
    d. CPU and RAM benchmarking testing
    e. Read/Write latency testing
    f. Data Replication Testing
    g. Firewall policy and configuration testing
    h. Data Integrity Testing
    i. Reverse Replication Testing
    j. Switch over testing
9. The Government Department should ensure proper documentation is received from the CSP/ MSP and only then the Sign-off is handed over to the CSP/ MSP

9. Glossary of Terms

Acronym	Expansion
CSP	Cloud Service Provider
RFP	Request for Proposal
GeM	Government e-Marketplace
IT	Information Technology
MeitY	Ministry of Electronics & Information Technology
IaaS	Infrastructure as a Service
PaaS	Platform as a Service
SaaS	Software as a Service
PC	Public Cloud
VPC	Virtual Private Cloud
GCC	Government Community Cloud
NIC	National Informatics Center
CAPEX	Capital Expenditure
IOPS	Input Output Operations per Second
VPN	Virtual Private Network
MPLS	Multi-Protocol Label Switching
UI	User Interface
DC	Data Center
OS	Operating Systems
OEM	Original Equipment Manufacturer
IP	Internet Protocol
KPI	Key Performance Indicators
SLA	Service Level Agreement
IAM	Identity & Access Management
DB	Database
GB	Gigabyte
RAID	Redundant Array of Independent Disk
CPU	Central Processing Unit
TCO	Total Cost of Ownership
DR	Disaster Recovery
VM	Virtual Machine
H/w	Hardware

Acronym	Expansion
S/w	Software
N/w	Network
QA	Quality Assurance
I/O	Input Output
SSD	Solid State Disk
SAS	Serial Attached SCSI
SATA	Serial AT Attachment
NL-SAS	New Live SAS
IPS	Intrusion Prevention System
IDS	Intrusion Detection System
HIPS	Host IPS
SIEM	Security Incident & Event Monitoring
DLP	Data Leakage Prevention / Protection
DDoS	Distributed Denial of Service
STQC	Standardization Testing and Quality Control Directorate
API	Application Programming Interface
SI	System Integrator
BCP	Business Continuity Plan
PII	Personally Identifiable Information
PHI	Protected Health Information
GST	Goods & Services Tax
GOI	Government of India
EU	European Union
PSU	Public Sector Undertaking
ISO	International Organization for Standardization
NOC	Network Operation Center
SOC	Security Operation Center
ITIL	Information technology Infrastructure Library
TIA	Telecommunications Industry Association
Mbps	Mega bits per second
Gbps	Giga bits per second
SPOC	Single Point of Contact

Annexure 1: Risk Assessment

Risk Assessment is a key activity when planning to migrate the application on Cloud. Assessing the application across various dimensions, such as geographical location of the data, sensitivity of data, business criticality, the need to protect personal identifiable information (PII) and personal health information (PHI), shall help a Government Department analyze the risks associated and if the Government Department can migrate its application on Cloud with the risk or if any mitigation plan is required to be formulated to minimize the impact of those risks. The Risk Assessment table details various dimensions along which the risk to be measured, its description, guiding questions and their responses. Each dimension and its guiding question(s) may be modified by the Government Department in accordance to their requirements.

Dimension	Description	Guiding Questions	Response (Yes/No)
Cross Border Data/ Jurisdiction	The geographic path and location of the data managed by the application. The data should be hosted within Country / jurisdiction. Data crossing international borders is subject to specific laws as defined by Government of India.	If the answer is "YES" to any of the below, this risk applies. • Does application transact data that demands data sovereignty within the country/territory? • Are the application users crossing international borders to access this application or store its data? If the risk does not apply, continue. If the risk applies, continue by ensuring adequate security measures to mitigate the risk and address the challenges & gaps, post which the Government Department may migrate its application to Cloud.	
Regulated Data	The need to protect sensitive data from unauthorized disclosure, fraud, waste, or misuse (e.g. Government Financial Records, Sensitive Intellectual Property) Data regulated by specific country regulations such as Outsourcing of Business Activities, Functions and Processes.	If the answer is "YES" to any of the below, this risk applies. • Does application transact data that is regulated by the laws of the country e.g. Financial Reporting data, Aadhaar specific data. • Has the application data been classified across following categories: Top Secret, Secret, Confidential, Restricted, Public Data? • Does this require approval from the Department Heads / Competent Authorities? If the risk does not apply, continue.	

Dimension	Description	Guiding Questions	Response (Yes/No)
		If the risk applies, continue by ensuring adequate security measures to mitigate the risk and address the challenges & gaps, post which the Government Department may migrate its application to Cloud.	
Application Criticality / Availability	An application that is essential to supporting the core business processes of a Government Department. A failure or disruption of application may result in the failure of business operations or serious impact on the services offered by the Government Department.	If the answer is "YES" to any of the below, this risk applies. Is this application supporting a core business process and is application considered mission critical or strategic application? Are there limitations on moving the application to a cloud service provider with variable service availability? Will business continuity and recovery policies be impacted? If the risk does not apply, continue. If the risk applies, continue by ensuring adequate security measures to mitigate the risk and address the challenges & gaps, post which the Government Department may migrate its application to Cloud.	
PII/PHI Data	PII and PHI data is considered to be one of the most sensitive forms of data. It is essential for a Government Department to protect The Personally Identifiable Information (PII) and Protected Health Information (PHI) from unauthorized disclosure, fraud or misuse.	If the answer is "YES" to any of the below, this risk applies. • Does the application in the Government Department's environment transacts any PII or PHI data that is regulated by the laws of the country? • Does this require approval from the Department Head / Competent Authority? If the risk does not apply, continue. If the risk applies, continue by ensuring adequate security measures to mitigate the risk and address the challenges & gaps, post which the Government Department may migrate its application to Cloud.	
Reputation Impact	Negative impact on the reputation of a Government Department and its identity due to the	If the answer is "YES" to any of the below, this risk applies. • Are there any critical implications to the reputation of a Government Department if	

Dimension	Description	Guiding Questions	Response (Yes/No)
	failure of a 3rd party to provide the contracted services which were essential for citizens. (Primarily applies for citizen centric applications)	the Cloud Service Provider faces considerable downtime or the application data is compromised? • Is Indemnity against 3rd party intellectual property infringement required? If the risk does not apply, continue. If the risk applies, continue by ensuring adequate security measures to mitigate the risk and address the challenges & gaps, post which the Government Department may migrate its application to Cloud.	
Licensing	It defines the licensing requirement of a Government Department. Different Middleware, Database, Backup license(s) etc. might be required to run the applications. Licenses may be restricted in use based on CPU, virtualized hosts, concurrent users, ability to transfer, etc. (Licensing policy)	If the answer is "YES" to any of the below, this risk applies. • Do licenses need to be managed to ensure compliance in a cloud environment? • Do licenses disallow for elasticity / horizontal scaling across additional hosts? • Does enterprise agreement need to be updated or renegotiated for leveraging licenses at cloud service provider location? If the risk does not apply, continue. If the risk applies, continue by ensuring adequate measures to mitigate the risk and address the challenges & gaps such as: In case of managed license requirement or requirement of modification of license agreement to use licenses on cloud, the Government Department may use services made available from the Cloud Service Provider. Hence by ensuring certain measures Government Department may migrate its application to Cloud.	

Annexure 2: Strategic Alignment & Cost Assessment

Strategic Alignment and Cost Assessment is another key area for Government Departments to analyze before migrating its application to Cloud. It is essential to understand for Government Department which Cloud Deployment Model and Cloud Service Model shall be suitable, the total cost of ownership for migrating to cloud and running business operations successfully from the chosen Cloud. Each dimension and its guiding question(s) may be modified by the Government Department according to their requirements.

Dimension	Description	Guiding Question	Response (Yes / No)
Strategic Fit	Most suitable strategy adopted for selection of Cloud Service and Deployment model	• Is the time required for migrating your applications to Cloud, high? • Can the existing environment of a Government Department not be replaced by the services offered by the Cloud Service Providers If the answer to any or all of the question(s) is 'No', the application is technically feasible to migrate to Cloud If the answer to any or all of the question(s) is Yes and the Government Department must ensure measures such as: • In case the time for migration of application is high, the Government Departments must plan the application migration as per the migration roadmap (elaborated in section 7.2) • Evaluate alternatives made available through Cloud Service Providers for services which cannot be replaces. Post ensuring adequate measures the Government Department may migrate its application to Cloud.	
Cost Fit	Cost factors related to migrating and operating the application in the cloud	• Is the Government Department not aware of Cost to re-factor the application and level of investment required to refactor legacy components to leverage service capabilities offered by Cloud Service Provider?	

Dimension	Description	Guiding Question	Response (Yes / No)
		• Is the Government Department unaware of the cost to consider migrating its own current setup to Cloud or leveraging equivalent services from the Cloud Service Provider platform? If the answer to any or all of the question(s) is 'No', the application is commercially feasible to migrate to Cloud If the answer to any or all of the question(s) is Yes and the Government Department must perform proper cost assessment and price discovery of services post which they may migrate their application to Cloud.	

Annexure 3: Migration Template (Indicative)

Phase / Task No	Task	No. of Servers	Estimated No. of days for migration	Estimated Downtime (No. of Hrs)	Remarks
Phase-1	**Establishing Connectivity**				
1	Setting up of Internet Connectivity & Testing				
2	Setting up of MPLS Connectivity & Testing				Dependency on BSNL / any other service provider
Phase-2	**Network Security**				
1	Configuration of WAF / Firewall, Security Parameters, Site to Site VPN, etc				
2	Testing				
Phase-3	**Server Migration**				
Phase-3A	**Migration of Production & Critical Server and Testing**				
1	Active Directory and DNS				
2	Terminal Server Gateway and Terminal Server				
3	Web Server (IIS)				
4	SQL Database Server (Web Database)				
5	Application Servers				
Phase-3B	**Migration of Non – Critical Servers**				
1	Application and Database Servers				
2	File Server				
3	Ant Virus				
Phase-3	**Migration of DEV/UAT/STAG and other servers**				
2	Web Development Servers and Database Server				
3	UAT and STAGING Servers				
	TOTAL	**0**	**0**	**0**	
Phase-4	**Disaster Recovery Site Setup & Readiness**				
1	DR Drill				DR Drill execution for 7 days(apx)
Total Estimated No. of Days for Complete Migration to Cloud DC, setting up of DR site on Cloud and executing DR Drill			**0**		

Annexure 4: Productization of Application

Productized and Cloud enabled applications are ideal solutions that can be utilized by various departments at center and states without having to invest time, cost and effort in development of the same. This would enable re-use and deployment of applications rapidly across several states/departments

Need for Software Development & Re-Engineering Guidelines

The basic need for Re-engineering is to ensure development of Common Application Software (CAS) which can be configured as per different states / departments requirements without the need of modifying the core code of the application for a faster deployment so that time, effort and costs in developing applications are saved and to obviate duplication of efforts. It is therefore imperative that applications are developed in conformity to guidelines that makes them standardized and compatible for hosting and running across states. This need has translated in the conceptualization, development and roll-out of productized cloud enabled application which can be centrally run & hosted and are available to states for configuring them as per their relevant processes with minimal customization for rolling out the services in shortest time possible.

It is envisioned that an application which is centrally run as a SaaS is easy to roll out to all interested parties at the same time and therefore such application's architecture and design should be compliant to common minimum practices / considerations that will convert it to standard product.

Software Development and Re-engineering

The solution architecture is key differentiator for product like solutions. A well architected solution gives it robustness for reusability (in code, configurations, databases, services etc.), enhancements and interoperability.

The following should be adopted as good architecture principles:

1. **Well established Service Contracts:** A contractual agreement between the Application Owner (Govt. Department at Centre/State or any Private Player) and the Application Provider (Govt. Department or independent entities which host & provide services through eGov AppStore) over the period of Application Lifecycle (for example: Productization + Replication + Hosting + Operation & Maintenance). The contracts related to licenses, source code etc. will also be a part of such agreements.
2. **Loose Coupling of Services:** This is one of the fundamental concepts of Service Oriented Computing. Loose coupling ensures that application components are treated individually and dependencies are reduced. This further ensures that addition, removal, failure or update of one component has a minimum impact on other components. Effort should be made to develop components separately and then their integration/ interaction mechanism could be defined in a separate component. For example, while

developing a component that calculates the order of a commodity should not start calculating the total cost of the order placed. Order should be calculated separately and the cost should be calculated separately so that any change in costing structure should only affect the cost calculation code and not the order placement component.

3. **Service Reusability:** For the purpose of reusability, services should be written in such a way that they can be automated for testing. Test automation is necessary to ensure services can be upgraded, re-factored, etc. without breaking other services that use this. Further, all services should be inherently versioned and all invocations must specify the version of service. Efforts should be made to ensure that new versions of services should be backward compatible with at least one or two previous versions so that users of the service can start using new version of the service without mandatorily making changes to their code. Rapid Replication and productization of successful applications running across different States/UTs would ensure that these applications are also reusable in other states with appropriate built-in configurations which can be undertaken by concerned seeker state / department. The solution should also support minor customization if so essentially required by the seeker state / department. Software components can often be classified according to reusability levels:
    - **Foundation Components** - Examples of foundation components are classes such as Money, Date, List, Person and Number. These can be reused in almost any application
    - **Domain Components** - Examples of domain-specific components include classes like Customer, Account, and Transaction
    - **Architectural Components** - Examples of architecture-specific components include event notification mechanisms; user interfaces components, and message passing systems
    - **Application Components** - Examples of application-specific components include message handlers, exception handlers, and views
4. **Service Abstraction**: Abstraction provides control on what part of the service logic of a particular application are private (hidden) and what parts are made public (consumable). The public or consumable parts of the service logic can be designed in a generic manner to ensure that they encourage reusability as discussed in the point above. Abstraction also supports the loosely coupled principle discussed above. In a three tier (database, business and presentation) software application, necessary abstractions should be done in each layer so as to achieve loose coupling and to keep the code modular so that addition of any logic could easily be done at any tier.
5. **Service Discoverability**

    It is important that accidental creation of redundant services or implementation of redundant logic is avoided. Service discoverability ensures that metadata is attached

to a service and describes overall purpose of the service and its functionality, which makes the services easily discoverable.

6. **Service Autonomy:** It is important to ensure that services which are delivered do not just possess reusable logic, but they are also autonomous to be reused. This Autonomy will also facilitate adaptation to changing constraint in terms of scalability, service levels adherence, availability etc. For example only loosely coupled services or service components can be reused, therefore autonomy becomes an important parameter to efficiently design solutions.
7. **Service Location Transparency:** This refers to ability of the Service Consumers to use a service regardless of its actual location, for example being available on a cloud.
8. **Service Granularity:** Service Granularity means identification of optimal scope of business functionality in a service operation. Each service operation should ideally perform single transaction to simplify error detection, error recovery, and simplify the overall design (this means that particular Service operation is granular). In addition, each service operation maps to a single business function, although if a single operation can provide multiple functions without adding design complexity or increasing message sizes, this can genetically reduce implementation and usage costs.
9. **Platform & Database Agnostic:** From an architectural perspective, it would be required that the productized solutions should be not only be modular in nature, but be adaptive to converse with other technology components such as platforms and databases, complete with management suites or with the induction of adaptors and interfaces or even smaller bespoke solutions to support the same. It would also be required that the application provider should be able to deliver application on latest IT Infrastructure & system software components available at National Cloud and at SDCs under Meghraj. This would ensure that the applications developed can overcome the technology dependences and be available to a variety of seeker states
10. **Application design for occasionally connected systems:** For the small percentage of functionality that requires "occasional disconnected/offline" operations, applications may be designed to use a local persistent store/cache just for the purposes of offline capability and later sync as and when connectivity is restored. As connectivity becomes ubiquitous, less of such offline capabilities are needed.

Standards Adoption & Solution Engineering

There are a number of standards available on software engineering lifecycles which ensure quality product development and scope of continuous improvements. The standards are to be followed as per the Government of India issued policies and guidelines promulgated from time to time. The proposed solutions should be adaptable to the following as good software engineering practices:

1. **Domain / Sector specific Meta Data Standards:** Each sector or domain has its unique challenges in standardization of Meta-Data. It is important that any solution being developed to provide services in the domain or sector adhering to the Meta-Data standards for that particular sector or domain. This would ensure seamless integration between solutions developed for domain or sector. The GOI has also come out with Meta data standards which can be seen at www.egovstandards.gov.in
2. **Software Engineering Standards:** It is important that software engineering standards are adopted during the initial stages of the development lifecycle to ensure that the developed solution is able to meet quality certifications and security testing. Recommended testing requirements will be provided by STQC / empaneled agencies.
3. **Usage of Open Standards technologies:** As part of the software engineering, it is important to use technologies developed in open standards. As part of the overall software development lifecycle, a minimum customization and maximum configuration approach should be adopted. There should not be any hard-coding in any aspect of the development and release lifecycle of the proposed application. The following section articulates areas (no limited to) that should be available as configurable parameters, while overall software having the ability to be customized so as to meet the local requirements of the user state / department / agency. e-Governance application should preferably be developed using open source tools and components.

Configurable Components

An important facet of product like solution is its ability to be configurable to meet the business requirements. The following should be available as configurable components:

1. **Master Data:** Master data should be available in parameterized format. It should be based on the Meta data standards for the industry / domain / sector. They should not be hard-coded in the application.
2. **Screen Labels:** Screen labels may differ between solutions owing to the localization requirements for a solution proposed to be implemented. Configuration of screen labels should be made available through resource files. They should not be hard-coded in the application.
3. **User Alerts & Messages:** Based on the Government Departments business requirements, alerts and messaging services need to be pushed or pulled to the end user. Allowing for alerts and messages to be available as a configurable component would ensure that unwanted alerts and messages are not routed through to all workflow entities.
4. **Reports:** It is generally required from solutions to be able to prepare various kinds of reports for various levels of officers in the hierarchy, along with aggregation and data sorting features. Available as a configurable component, it would ensure that the

reports are localized to the needs of a user, rather than being generic to business function or sub-unit.

5. **Workflow Management:** Common business functions in two similar organizations may have different processes related to approvals, escalations, reviews, recommendations etc.; therefore, it is important that workflows are available as configurable components to allow the solution to be configured to the business requirements of that organization.
6. **Multi Language Support:** Government departments operate in multiple languages depending on their region. Product like solutions should be adaptable, to allow through configuration, selection of language in which the user wishes to operate the system. Product like solutions should at least be bi-lingual, with English as one of the languages.
7. **Business Rules (if - then - else):** Business rules are at the core of workflow processes and allow for information, interaction and transaction services to be communicated. Product like solutions should ensure that business rules are configurable to allow the organization to localize the solution to their business requirements. They should not be hard-coded in the application.
8. **Dashboards:** As a management tool, most senior officers require dashboards to review service progress, service levels, escalations, alerts and reminders, messages etc. As an operational tool it is required by the office staff for work-list detailing, alerts, reminders and messaging. As configurable component, it would ensure that the user is able to see his or her, role-based dashboard for summary of tasks and activities to be completed.
9. **Online Help & Feedback:** As a feature in most standard products it would be required that online help and feedback mechanism should be available as configurable parameters to assist the users in functioning of the application. This could include context sensitive help, user manuals etc. In online feedback mechanism, feedback on technical aspects as well as service delivery should be given to the users.

Customizable Components

A solution may be required to be customized to meet specific business requirements of an organization. The following should be kept in perspective while customizing core solutions:

1. **Ability to add additional features without compromising the core code** The solutions should be developed in modular format, or should allow for modular integration or interfacing with other solutions, without the need of editing existing core code. Solutions should allow for the development of new features, functionalities, changes to done through interfaces external to the existing code base.
2. **Ability to interface with other independent sub-applications** It may be required that a product like solution is required to interface with other bespoke smaller

applications, unique to an organization. There should be minimal effort required for such activities and should be made available through external adaptors interfacing with the core application. Methods of customization include:

a. Implementing a plug-in architecture so that tenants could upload their own code through defined interfaces without changing the core application or;

b. Using some form of rules engine that enables process customization through configuration

c. Another alternative to consider is enabling application to call a service endpoint provided by the tenant, which performs some custom logic and returns a result. In addition, application may also require providing ways to extend the application without using custom code. To achieve this application must implement a mechanism for customizing the UI, and a way of extending the data storage schema. Methods of extending schema can be:

    i. Single fixed schema with a set of columns available for custom data

    ii. Single fixed schema with separate tables holding custom data

Solution Sizing & Scalability

Since the solution will be required to be hosted on various deployment models, it is important for the solutions to be able to scale up to meet increasing usage requirements. Although an initial estimation of the hardware specifications (quantity and model / version) would be required to size the solution based on system interaction, to increase capacities the solution should adaptable to scaling. The following should be kept in perspective:

- **Able to scale up to meet increasing load -** Solution should be able to handle increasing number of first-time users, transactions, data sharing processes etc.
- **Able to demonstrate stress levels exerted -** Solution should be able to handle increasing number of concurrent users, concurrent transactions, synchronous data sharing with other systems etc.
- **Able to perform on throttled bandwidth environments** - Solution should be able to perform to the agreed service levels regardless of the bandwidth available or in multiple bandwidth availability scenarios
- **Should have low technical & infrastructure resource consumption** - Solution should optimally use technical resources such as memory, processor (CPU), storage etc. In addition, should optimally use data center resources on available bandwidths.
- **Should be interoperable to newer technology upgrades -** The solution should be able to harness the advantages of legacy technology (servers, software, devices etc.) while be able to upgrade to newer systems. This would enable low cost – optimal utilization of resources.
- **Horizontal Scalability:** Scalability of an application is aided through designing services as granular as well as loosely coupled. Use of distributed data stores and

sharding also aid application scaling. If the service uses database/data store, it must ensure database layer can also span multiple database nodes. his can be achieved either by using a distributed data store; or

If using traditional RDBMS systems, this can be achieved by ensuring application level sharding (partitioning) is implemented to partition data across many RDBMS nodes. Each shard has the same schema but holds its own distinct subset of the data. A shard is a data store in its own right, running on a server acting as a storage node

Language & Interface

A key requirement for government application being available nationally is their ability to provide the user a local interface and support local language. Therefore, the proposed solutions should:

- **Be developed on Unicode Compliant Code practices** - The development should be undertaken using Unicode compliant practices.
- **Support open standards on language interfaces -** The solution should support open standards on language interfaces.
- **Should support multiple language (Indian & Foreign) APIs** - Solution should at least be bi-lingual but should possess capabilities to be multi-lingual.
- **Should support self-learning data dictionaries** - The solution should be support APIs that enable building of transliterated data dictionaries, with preemptive text, so that the user is given the choice to select the nearest match.

Legacy Integration – Digitization & Migration

The proposed solution should be able to acquire, sort and store the data that has been accumulated for the service being provisioned through multiple legacy ICT solutions. Therefore the proposed solutions should be:

- **Able to migrate data through offline user interfaces -** The solution should provide for manual data entry of legacy data (allow for conduct of digitization activities)
- **Able to migrate data through be-spoke / product utilities -** Solution should support migration legacy data through be-spoke utilities which allow for data entry, extraction and submission of data into the proposed solution 2.8 Intellectual Property Rights (for Center & State owned applications)

Intellectual Property Rights (for Center & State owned applications)

The Intellectual Property Rights for the developed product should invariably reside with the Government Department. This should include the source code, release management artifacts and all other technical and domain related documentation for the developed solution. The licenses procured for the implementation of the existing application may be provided.

- Release Management Artifacts should include, but not be limited to the following:

- Core Application
- Packaged Installation
- Application Code
- Code Review
- Unit Test Results (Multilingual)
- Test Suites
- UAT Scripts & Test Cases (Multilingual)
- User Interface Testing Results (Multilingual)
- Performance Test Results
- Security Test Results
- Requirement Traceability Matrix
- Deployment Scripts
- Deployment Manual
- User Manual
- Technical Manuals
- Release Notes
- Standard Operating Procedures
- Application Customization Guidelines
- Quality Assessment Report
- UAT Acceptance Benchmarks
- Mapping sheet for defects/functionality and system test cases
- Non-Functional Requirements Compliance sheet
- Backup of the Database before executing the incremental Script
- Incremental Script
- Release note for Database changes done between builds
- DB Code Review Report

The IPR for the developed product / solution should not be restricted / compromised through any legal interpretation. The solution should clearly be the property of the government department.

Annexure 5: Resource Management Guide

This section of the document has been prepared to assist government organizations in referring to several Laws, Regulations, Guidelines and Standards while leveraging Cloud Services. This section begins with the Laws and Regulations currently in place in India. This section stipulates some of the Indian Acts, Rules and Guidelines under the legal ambit of which Cloud Computing services would fall, followed by some important Guides and their references, along with the Standards that must be known to the Government Departments.

The Government of India has made it mandatory, through Rule 149 of General Financial Rules 2017, for Ministries or Departments to procure goods and services through the GeM platform if they are available on it. Due to this, the empaneled CSPs have started offering their Cloud services on GeM. Since then, some Government Departments have already procured the basic Cloud infrastructure packages. However, while leveraging any Cloud Services from the CSPs, it is necessary for the Government Department to be aware of the Laws, Regulations, Guides and Standards that they must refer and adhere to. It is in the above context that this section is prepared to provide details on such resources.

References at Glance

The Government Departments may refer to the below mentioned Laws, Regulations, Guidelines and Standards when leveraging Cloud Services:

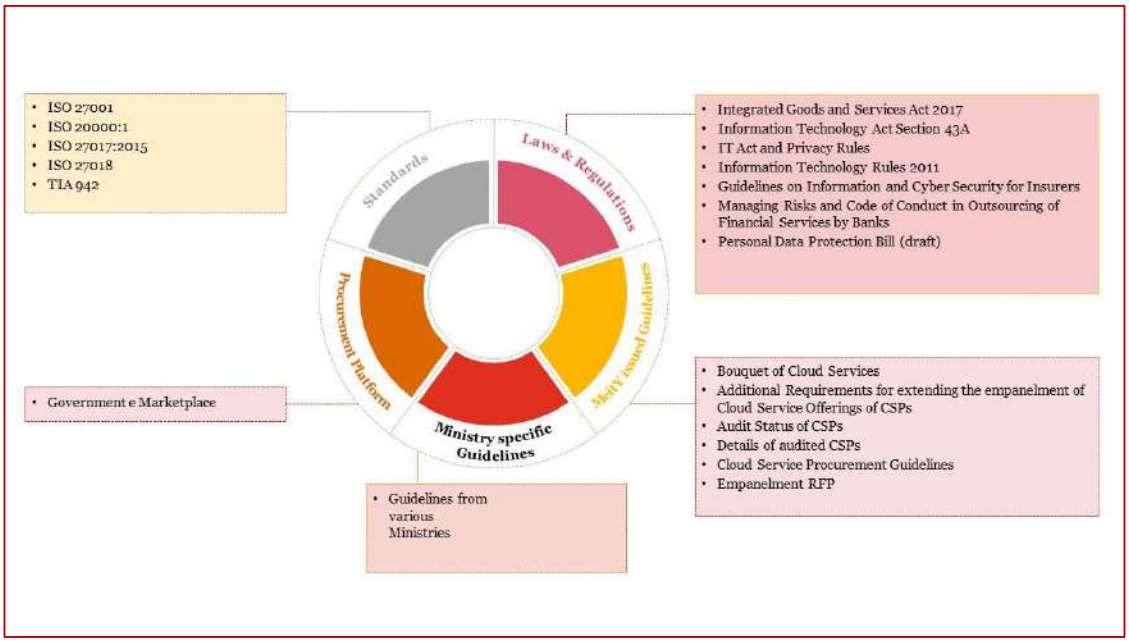


Figure 18: Resource Reference Summary

Laws and Regulations

The Cloud Computing services would fall under the legal ambits of following legislations:

- 'Cloud services' are recognized under the **Integrated Goods and Services Tax Act 2017** (the GST Act) under 'online information and database access or retrieval services' and therefore the services rendered by Cloud Services Providers would be subject to GST.
- **Information Technology Act Section 43 A** and the Reasonable Security Practices and Procedures and Sensitive Personal Data or Information Rules 2011 (the Privacy Rules) under Information Technology Act provide guidelines for collection, use and protection of the sensitive personal data or information of persons by a body corporate that possesses, deals with or handles such data.
- The **IT Act** and the **Privacy Rules** together set out the regulatory framework for creation, collection, storage, processing and use of electronic data (including personal and sensitive personal information recorded in electronic form) in India.
- CSP's in India would also need to follow the principles of the **Information Technology (Intermediaries Guidelines) Rules 2011** and (Intermediary Guidelines) under the Information Technology Act.
- Government of India has drafted a **Personal Data Protection Bill** and the same once notified will overhaul the existing framework of privacy and data protection regime in India. The Bill is in many respects similar to General Data Protection Regulation, EU and it, inter alia, enhances the stringency of obligations and corresponding penalties governing data protection from a customer perspective.
- In addition to the IT Act and Privacy Rules, the use of Cloud Computing in the banking and insurance sectors is subject to specific restrictions. The RBI's guidelines on **Managing Risks and Code of Conduct in Outsourcing of Financial Services by Banks** read along with the **Report of Working Group of RBI on Electronic Banking** set out specific requirements to be complied with by banks while engaging Cloud Service Providers. These requirements, inter alia, relate to vendor selection, data security, form of agreement, business continuity and disaster recovery or management practices.
- The Insurance Regulatory and Development Authority of India's (IRDAI) **Guidelines on Information** and **Cyber Security for Insurers** require insurers to comply with requirements, inter alia, in relation to data, application and network security, incident management, and information security audit while using services from a Cloud Service Provider.
- On August, 24th, 2017, a nine-judge bench of the Supreme Court of India conclusively held that the right to privacy is a fundamental right guaranteed to the citizens of India (subject to reasonable restrictions).

- The government retains the authority to intercept any information transmitted through a computer system, network, database or software for the prevention of serious crimes or under grave circumstances affecting public order and national security. The **Ministry of Home Affairs** has passed an order "authorizing" ten central agencies under Section 69(1) of IT Act, 2008, read with Rule 4 of IT Rules, 2009, for the " ……purposes of interception, monitoring and decryption of any information generated, transmitted, received or stored in any computer resource…"

MeitY Issued Guidelines

The Government Departments can refer to the various documents / guidelines available on https://meity.gov.in/content/gi-cloud-meghraj but not limited to:

- **Bouquet of Cloud Services (Cloud Guidelines):** The Cloud services, listed under this section, have been categorized into "Basic Cloud Services" and "Advanced Cloud Services". The Cloud services listed under the "Basic Cloud Services" are mandatory for all CSPs to offer to the Government Organizations under at least one of the empaneled Cloud Deployment Models. However, the Cloud services listed under the "Advanced Cloud Services" category are optional for the CSPs to offer.
- **Additional Requirements for extending the empanelment of Cloud Service Offerings of CSPs:** These are the additional empanelment requirements for the existing Cloud Service Providers empaneled by MeitY in 2016 and 2018.
- **Audit Status of CSPs:** This list represents the current audit status of MeitY empaneled and STQC audited CSPs
- **Details of audited CSPs:** This list represents the empaneled Cloud Service offerings and deployment models of the empaneled CSPs

Cloud Service Procurement Guidelines (Cloud Guidelines): MeitY has issued documents to help the Government Departments and PSUs in procuring Cloud services from the empaneled Cloud Service Providers. The Government Departments can refer to the documents like procurement guidelines, Service Level Agreements and contractual terms/ Master Service Agreement while leveraging Cloud services. These documents are meant to provide an indicative direction and they can be suitably modified/ aligned as per individual Department's requirements.

Standards

As per the empanelment requirements and guidelines for Cloud Services, the CSPs are required to ensure that their services must comply with the below standards:

- **ISO27001** - The Data Center should be certified with the latest version of ISO 27001 (year 2013) and provide service assurance and effectiveness of Management.
- **ISO20000:1** - The NOC and SOC facility must be within India for the Cloud Environments and the managed services quality should be certified for ISO 20000:1.

- **ISO27107:2015** - CSPs should comply with latest Cloud Security ISO Standard ISO 27017:2015 and Privacy Standard ISO 27018:2015.
- **TIA942** - The Data Center should conform to at least Tier III standard (preferably certified under TIA 942 or Uptime Institute certifications by a 3rd party) and implement tool-based processes based on ITIL standards.

Procurement Platform

All the Government Departments must be aware of the GeM platform as they must procure any empaneled Cloud Services through GeM. The CSPs offer the empaneled Cloud services to government organizations through GeM. CSPs whose Cloud services are successfully empaneled with MeitY shall onboard these services on the GeM platform as per the directions provided by the GeM team. Government organizations may procure these empaneled Cloud services from the GeM Marketplace or through the Bid / Reverse Auction facility available on the GeM platform.

Ministry Specific Guidelines

There are several Ministries that issue various data retention guidelines as per their requirement. For example, the Income Tax Ministry has a retention policy of 7 years. While leveraging Cloud Services, the Government Departments should also refer to these guidelines issued by specific Ministries.

Annexure 6: Checklist for Migration

S. No	Task	Status	Remarks
1.	Has the Application Readiness Assessment been performed by the Government Department?	☐	
2.	Has the utilization report for existing IT System in terms of compute been studied?	☑	
3.	Has the utilization report for existing IT System in terms of Storage (consumption, IOPS) been studied?	☐	
4.	Has the utilization report for existing IT System in terms of bandwidth (in Mbps/ Gbps) been studied?	☐	
5.	Has the Government Department carried out technical Feasibility of application to be migrated to Cloud?	☐	
6.	Has the Government Department carried out Risk Assessment of application to be migrated to Cloud?	☐	
7.	In consideration with the MSP and the SI has the Government Department prepared sizing template for cloud?	☐	
8.	Has the Application Dependency Matrix/ document prepared for the project?	☐	
9.	If further optimization in capacity sizing possible, then, has the consolidation assessment, been performed by the Government Department?	☐	
10.	Has the Government Department prepared a migration strategy for the entire project?	☐	
11.	Have the timelines for migration been identified by the Government Department?	☐	

S. No	Task	Status	Remarks
12.	If the timelines for migration have been identified have the same been documented by the Government Department?	☐	
13.	Has the MSP in consideration with the CSP submitted a Technical Architecture and Design Document for the project?	☐	
14	Have certain tools and platforms been identified by the Government Department in consultation with MSP/CSP to facilitate the migration activity?	☐	
15.	Have a project SPOC (Single Point of Contact) been appointed by the Government Department?	☐	
16.	Have various Test Cases been identified and documented by the Government Department?	☐	
17.	Has the migration environment been created on Cloud?	☐	
18.	Has the Internal staff of the Government Department provided training on Cloud Management Portal of the CSP?	☐	
19.	Has the Government Department taken system backup before Migration?	☐	
20.	Has the Downtime window decided and approved by the Government Department?	☐	
21.	Has the Government Department defined Backup & Retention Policy?	☐	
22.	Has the connectivity been established between Government Department and Cloud?	☐	

S. No	Task	Status	Remarks
23.	Has the Government Department identified Security Controls applicable on CSP in addition to the one's outline by MeitY w.r.t project specific requirements?	☐	
24.	Has the Government Department performed Data Integrity checks post migration?	☐	
25.	Has the Government Department performed Application, Functional and User Acceptance Testing post migration?	☐	
26.	Have the Production Application and Database servers restored on the Cloud Platform?	☐	
27.	Have the application and database configuration been performed by the CSP / MSP as per roles & responsibilities outlined, on the Cloud post migration?	☐	
28.	Has the Government Department handed over any software licenses to the CSP / MSP under the BYOL terms?	☐	
29.	Has the Government Department conducted DR drill (as applicable), post migration to Cloud?	☐	
30.	Have the migration formalities completed by stakeholders and final signoff handed over to the CSP / MSP?	☐	