Annexure A

Idea Cellular Response to TRAI Consultation Paper

On

"Cloud Computing"

Introduction

At the outset, Idea Cellular welcomes the opportunity to contribute to this Consultation paper. As you would acknowledge, the TSP with their inherent ubiquitous network and coverage, are best positioned to provide the platform for cloud based services and applications.

The advancements in Cloud Computing technology enables business units to deploy compute resources quickly and scale up as required at lower costs. Cloud computing also enables businesses to use the "ready to use" scalable service platforms.

The advantage of cloud computing to the data driven industries is significant, especially to the SME's. Indian businesses, primarily those operating in the telecom, Banking & Financial Services (BFSI), insurance, education, and governance sectors are rapidly deploying cloud computing applications that promises them access to convenient, on-demand network by a shared pool of computing resources placed in scalable data centers. **However, the standards available in the cloud industry are sparse and there are no single standard available. This creates interoperability issues. TRAI should take note of this issue and ensure that a minimum set of guidelines are formed. It should also ensure that these do not in any way hinder the adoption of cloud.**

While the popularity and usage of cloud computing is fast picking up, we would like to bring to the attention of TRAI, a couple of important areas that need to be focused, specifically on telecom operators issues, to enable adoption of cloud technologies in holistic manner :

- **The telecom licenses have certain restrictive clauses which inter alia leave uncertainty for the TSPs to leverage the benefits of cloud services for/on behalf of their customers.**

- **Typically, the license restricts the telecom operators to share any user identifiable information outside India. This is creating reluctance and uncertainty in TSPs to avail the benefits of cloud for their subscribers. However, similar or more information pertaining to identification of the subscribers is being sent outside India through subscribers themselves or through handsets or websites. This situation leaves TSPs at disadvantage.**

- **Considering that the provisions of the Information Technology Act are already applicable to the TSP, we submit that no separate provision in the license is necessary.**

- **We strongly recommend that the framework which TRAI endeavors to formulate after this consultation should ensure that the guidelines thus formed enable Telcos to promote agility, lower costs and interoperability with sufficient protection to the consumer and the cloud provider**.

In view of our above submissions, below is our query wise response:

Question 1. What are the paradigms of cost benefit analysis especially in terms of:

a. accelerating the design and roll out of services

b. Promotion of social networking, participative governance and e-commerce.

c. Expansion of new services.

d. Any other items or technologies. Please support your views with relevant data.

Idea Response:

The endeavor of an IT setup in an organization is to ensure that services are available, scalable and new services are rolled out quickly. The traditional model of IT delivery hinges on the concept of "On-premise" IT infrastructure. This IT infrastructure is built on a budgeted capital expenditure year on year. There is also a heavy reliance on the availability of skilled support staff to ensure the availability (smooth operations) of services that run on such infrastructure. Some key issues in this regard are :

- **Cost of Availability**

  On demand scaling and live migration in a virtualized cloud setup enables high availability of services. The multi tenancy and virtualization allows the high availability costs to be shared across multiple customers, software, hardware and services cost. The elastic capabilities of

the cloud allow the customer to reduce cost on deploying excess capacity in order to make the service available for spikes in workload.

- **Cost of Scalability**

  On demand scaling is a key paradigm shift in cloud technology. This on demand scaling provides an organization to pay as the scale increases instead of the traditional method of planning and procuring capacity in advance.

  This on demand capacity also decreases the time to market and helps to respond quickly to competition. The design and rollout of services become very quick in comparison to the plan-procure-deploy model.

- **Cost of Maintenance**

  Sourcing and retaining the expertise in the organization by itself is a task to organizations. In a Cloud model, due to the scale of infrastructure and the breadth of the technologies, sourcing and retaining the experts is an easier task compared to the in house model. This allows for lesser spends on man power for maintenance and passing the responsibility to the cloud service provider.

As a Telecom Service provider of voice and data services to the customers, the needs of the customer for more and more digital services need to be satisfied. The Cloud era provides this opportunity of providing digital services (for example Video Transcoding as service in Amazon Cloud) with the right set of experts and infrastructure. The agility, scalability and reduced maintenance costs are likely to result in increased adoption of the cloud model, provided enabling regulation of geography and confidentiality clauses is introduced without further delay.

Question 2. Please indicate with details how the economies of scale in the cloud will help cost reduction in the IT budget of an organization?

Idea Response:

The constitution of an IT budget in an organization primarily comprises of :

1. **Planning and Budgeting of Assets to be procured in the financial year**

   Procurement of Assets has to be planned in advance and procurement completed before the actual load kicks in to prevent any disruption in services. In a cloud environment, the cost of the assets required to deliver the service is much less when compared to in-house costs, because of the following factors:

   a. "On-demand" capacity procurement on the Cloud, enables payment for actual usage instead of pre procured assets.
   b. Due to the multi-tenancy models, the cost of a physical asset is shared across multiple customers.

2. **Budget provisions for Operations and Support**

   The major IT spends on operational expenditure are towards power and labor costs. Cloud environment reduces the Opex as explained below:

   a. The PUE of the in-house setup will be higher than the PUE of the cloud environment due to the scale, better utilization levels of the infrastructure in case of cloud environment, thereby resulting in improvement of efficiency in case of a large data center.
   b. The cloud service providers located in smaller cities can operate at lower power costs.
   c. Due to homogeneity of equipment on a cloud setup, there is high degree of automation for repetitive tasks. Hence the server to person ratio is low (less skilled resources to manage more servers) thereby reducing man power costs.
   d. Due to the multi-tenancy models, the cost of man power is shared across multiple customers, hardware and services

   NOTE : Software license models, especially from large vendors need to evolve to take advantage and reduce costs for consumers. At this point in time, the software license models adopted by certain vendors do not favor the cloud deployment models

Question 3. What parameters do the business enterprises focus on while selecting type of cloud service deployment model? How does a decision on such parameters differ for large business setups and SMEs?

Idea Response:

There are four models of Cloud deployment namely:

- Private Cloud
- Public Cloud
- Hybrid Cloud
- Community Cloud

The parameters that exert influence on the deployment models are:

1. **Assets and Capex**

   Large Businesses have an IT setup ranging from server rooms to large data centers. They have assets that are already deployed and can be used for existing operations and rolling out new services with an incremental spend on capacity addition. They also have the capability to invest on the additional infrastructure as Capex. SME's on the other hand, may not have any IT setup or a small IT setup. They may not have large capital investments to procure infrastructure in advance. They may prefer to invest in incremental phases in line with the business growth. The ease of addition of asset or the ability to invest as Capex plays a role in large business's decision to move to a private cloud whereas SME's tend towards a public cloud.

2. **Volume of data**

   Volume of data plays a big role in deciding the type of cloud deployment model. SME's data volume starts with a small scale and gradually expands. Large enterprises already have huge volumes of data. It is a technical challenge to migrate large volume of data to a public cloud. The challenges associated with this migration are copying data to cloud, bandwidth requirements to migrate and operate and costs associated with the large volume of data. Reusability of the existing infrastructure need to be thought through. Hence it seldom gives a clear path for large enterprises operating on large volumes of data to move to a public cloud model.

3. **Integrations or Application dependencies on other systems**

   With the options of SaaS, PaaS models, SME's are on a ready-to-deploy services without any integrations or any other application dependencies. Large enterprises cannot easily move the complete existing setup to a cloud environment. Portions of existing setup or new services are

strategically moved to cloud. This gives rise to a hybrid model of cloud deployment. Although theoretically this sounds like a workable model, the challenges associated with this model are latency requirements, volume of data moving between the clouds and the security of inflight data between the clouds.

4. **Culture and Mindset of the organization**

   Since Large Business' may have an IT setup on premise, there exists a 'mind-block' in the team to move from on-premise to a cloud. This primarily arises from the fear of the unknown, fear of security of data, fear of losing the utility of expertise and fear of loss of roles. SME's do not have this fear and many are 'born in the cloud' enterprises. Hence SME's readily move to Public Cloud deployment models whereas large businesses tend to move towards a private cloud.

5. **Goals of the organization**

   When two or more organizations have a common goal and decide to share data to leverage their goals, community cloud is the preferred deployment model. This model is applicable for both large enterprises and SME's.

Telecom providers in general have a large in-house deployment due to the traditional deployment methods and the large volume of data. With the advent of cloud technology there is flexibility available to the telecom providers to develop a hybrid model. However, the data transfer between the environments coupled with geography restrictions is still a challenge which needs to be addressed.

Question 4. How can a secure migration path be prescribed so that migration and deployment from one cloud to another is facilitated without any glitches?

Idea Response:

Smooth migration between one cloud eco system demands that data is portable between the clouds and the systems are compatible.

- **System Portability:** For system portability to be glitch free, there has to be a minimum common level which the cloud service provider, has to conform to. The applications or the services which

are deployed on cloud has to be certified on this minimum level. The minimum level of system requirements are defined and maintained by a consortium defined by the cloud regulation framework.

Some examples of the minimum level definitions are:

Operation Systems: Windows Version X, Linux Version X with minimum patch levels Y
Virtualization: VMWare Version X, Power VM
Networking addressing portability: Support Software defined networks
Load balancers: Software – Supports round robin

- **Data Portability:** Data portability refers to the ease of porting data from one cloud to another cloud. Data porting is not a major challenge for IaaS as the data is controlled by the customer and the format of data is known. In the case of SaaS, the format of storing data is decided by the application used by the service provider and the customer has little control over the format.

  Case 1: When two service providers have the same SaaS: A Minimum level of conformation has to be defined for the SaaS, which the service provider has to comply. Data extraction procedure and format to be defined along with this minimum level. This ensures that the data is portable across the service providers.

  Case 2: When two service providers do not have the same SaaS: When there is unique service being provided by a service provider, there has to be a data definition document which specifies the format of data stored, data retrieval procedures and the format of data retrieved which is in a standard format like a csv or any delimited file.

In both the cases, the encryption of data while exporting from the cloud or importing into the cloud, has to be taken care and this needs to be ensured as a part of framework for Cloud Service portability.

Question 5. What regulatory provisions may be mandated so that a customer is able to have control over his data while moving it in and out of the cloud?

Idea Response:

Please also refer to our answers to Question 4 and 6.

Regulatory provisions may be mandated for the following areas

a) Compliance to System portability

b) Compliance to Data portability

c) Compliance to standards as described in response to query no. 6.

The Authority also needs to consider jurisdictional issues in this regard.

Question 6. What regulatory framework and standards should be put in place for ensuring interoperability of cloud services at various levels of implementation viz. abstraction, programming and orchestration layer?

Presently there are too many standards and framework in the Cloud world. Following table lists the standards available currently.

Cloud Computing Standards, Specifications and Certification Setting Organizations

Organization	Type	Name	Number of standards or certifications
ATIS	SDO	Alliance for Telecommunications Industry Solutions	7
CSA	Certif.	Cloud Security Alliance	6
DMTF	SSO	Distributed Management Task Force	6
ETSI	SDO	European Telecommunications Standards Institute	55
EuroCloud	Certif.	EuroCloud	1
GICTF	SSO	Global Inter-Cloud Technology Forum	4
IEC	SDO	International Electrical Commission	See note
IEEE	SSO	Institute for Electrical and Electronics Engineers	1
ISO	SDO	International Organization for Standardization	18
ITU-T	SDO	ITU Telecommunication Standardization Sector	19
NIST	Agency	National Institute of Standards and Technology	6
OASIS	SSO	Organization for the Advancement of Structured Information Standards	4
ODCA	SSO	Open Data Center Alliance	28
OGF	SSO	Open Grid Forum	5
SNIA	SSO	Storage Networking Industry Association	1
TIA	SSO	Telecommunications Industry Association	1
TMF	SSO	TeleManagement Forum	6
NOTE: Common with ISO.			

This makes interoperability of cloud services very difficult and leads to vendor lock-in. After analyzing the various standards and frameworks available at this point in time, the following areas need mandatory standards and a defined framework.

a) User Authentication
b) Workload Migration
c) Data Migration
d) Workload Management

User Authentication: defines how a customer or an end user gets into the cloud environment for transacting, development, testing, configuration or administration. Some of the standards available are:

Standard/Framework	Examples of Usage
Amazon Web Services identity Access Management (AWS IAM)	Eucalyptus
Oauth	Force.com, Google app, Microsoft Azure
OpenID – Open standard for users to be authenticated in a decentralized manner	Google app, Microsoft Azure

Work Load Migration: defines how to move a workload in and out of a cloud. Some of the standards available are:

Standard/Framework	Examples of Usage
Amazon Virtual Image	Eucalyptus, Open Stack
Open Virtualization framework	Amazon EC2, Openstack , Eucalyptus
Virtual hard Disk	Amazon EC2, Microsoft Azure

Data Migration: defines the framework to move data in and out of the cloud. Some of the available standards are

Standard/Framework	Examples of Usage
Cloud Data Management Interface (CDMI)	
SOAP	Amazon EC2, Openstack , Eucalyptus
REST	Amazon EC2, Eucalyptus, Microsoft Azure, Openstack, Rackspace, Force.com

Work load management: defines the framework for interfaces to manage the work load

Standard/Framework	Examples of Usage
REST or SOAP	Amazon EC2, Eucalyptus, Microsoft Azure, Openstack, Google app engine, Go Grid

The Authority also needs to consider jurisdictional issues in this regard.

Question 7. What shall be the QoS parameters based on which the performance of different cloud service providers could be measured for different service models? The parameters essential and desirable and their respective benchmarks may be suggested.

Idea Response:

The following table gives a suggestion of parameters for measuring the quality of service of cloud providers:

Sr. No.	Area	Suggested parameters
1	Availability	Uptime guarantee of services and components. For eg For Iaas, uptime guarantee of the servers, storage. Maximum time allowed for a single outage Mean time to recover Number of outages Mean Time between failures
2	Performance	Response times. For eg in SaaS, response time for executing a transaction. Response time for provisioning a resource on cloud (like server , database, etc) Response time for on demand scaling For Iaas, response time for Server, storage , network
3	Service Management	Incident Response time Incident Resolution time

		Root cause analysis response time Failed changes Unauthorized changes
4	Security	Compliance Number of security breaches Compliance on PEN and Vulnerability tests Number of Denial of Service (DoS) attacks Audit
5	Exit Provisions	Time to consistently port out data – without disruptions to the service Time to clean wipe the data

Benchmarks are not provided as a part of this table due to lack of data points for these parameters on a cloud setup.

At this nascent stage of evolution of cloud services, it is suggested that no mandates on QoS should be given, and the same should be allowed to evolve based on free play of market forces. The Authority also needs to consider jurisdictional issues in this regard.

Question 8. What provisions are required in order to facilitate billing and metering re-verification by the client of Cloud services? In case of any dispute, how is it proposed to be addressed/ resolved?

Idea Response:

Billing and Metering is a core and mandatory component of a cloud service. We recommend:

a) The Cloud service provider should be able to produce consistent reports that are verifiable through audit of the respective systems.
b) The systems used for billing and metering should be a certified tool.
c) Retention period of Billing and metering data to be defined in the framework for cloud service.

It is suggested to have a Grievance cell to accept complaints on billing and metering and address them in a time bound manner.

Question 9. What mechanism should be in place for handling customer complaints and grievances in Cloud services? Please comment with justification.

Idea Response:

It is suggested to have a Grievance cell to accept complaints and address them in a time bound manner be framed. However we also submit that approach to grievances should not be harshly prescribed ,but driven by market forces in these competitive market.

Question 10. Enumerate in detail with justification, the provisions that need to put in place to ensure that the cloud services being offered are secure.

Idea Response:

It is submitted that security in a cloud environment needs to cover the following major areas:

1. **Cloud Model**

   The security provisions vary depending on the cloud model. SaaS is a software designed for the web and accessible to the end users. Examples include Gmail, Facebook. The application is designed for a specific purpose and does not offer much customization. This could lead to exposure if the cloud provider does not update his software regularly in line with regulations and vulnerability. In Iaas the infrastructure is a shared resource. Hence adequate controls need to be in place for protecting the provider as well as the customer.

2. **Access Policies**

   Access policies needs to be strictly governed, as irrespective of the cloud model, these resources are shared across the customer. Policies need to clear on who has the access to the data and how they will access it.

3. **Data**

The Data in the cloud can be stolen or can get corrupted. Provisions need to be in place to protect the data. Identity theft and stolen banking information or health records is common. The type of data also determines what kind of secure measure need to be put in place. For example PCI-DSS (Payment Card Industry data security standard) is required if the data has credit card information or banking related information. The storage and access of data is of prime consideration. Encryption methods needs to be adequate for data at rest and also for data in transit. To ensure availability of data appropriate backup plans need to be in place.

4. **Layers of Protection**

Controls and policies need to be in place for all the layers of the cloud service which are listed below

i) Facilities : Physical security and access to the environment

ii) Systems: Access controls and policy for firewalls, anti-virus, routers, switches, servers, storage, load balancers, etc.

Cloud service providers need to be certified on at least on one security standards depending on the geography. For example ISO 27001, SOC, PCI-DSS, etc.

Finally, on an overall level, it is critical that the approach to cloud regulation fosters support for new and innovative business models.

Question 11. What are the termination or exit provisions that need to be defined for ensuring security of data or information over cloud?

Idea Response:

Whenever the customer choses to exit the cloud by choice or due to cloud provider ceasing to provide the services, the following minimum provisions or guidelines needs to be ensured:

1. The data has to remain with (or transferred to) the actual owner of the service
2. No form of data either main or derived, should be allowed to be withheld by the cloud provider (after confirmation of the service provider that the data has been successfully transferred to other Cloud service provide or the service owner)
3. All backup copies of data to be deleted / purged by the Cloud Service Provider

4. The complete data (main and derived) has to be ported out of the cloud and the data has to be made available in a format that is available with the replacement Cloud Service provider.
5. In the event of acquisition of a cloud service provider, the provider cannot reassign the data to the new provider without consent of the customer.

Question 12. What security provisions are needed for live migration to cloud and for migration from one cloud service provider to another?

Idea Response:

Live migration is defined as the movement of the application or the workload to another machine either for availability or scalability. This scenario is particularly applicable in a virtualized environment where live applications are moved across VMs (Virtual Machines). From a security perspective, following are the points to be considered:

1. Availability of compliant and adequate resource
   The target VMs should meet all the defined security compliance and have adequate capacity so as to ensure availability of the service.

2. Network connectivity and associated access controls
   While moving from one VM to another, the network addressing scheme changes. All the firewall rules, access controls and bandwidth definitions should be taken care as to ensure the compliance like the source VM.

3. Encryption of data while moving from one VM to another

   Encryption mechanisms to be followed during a VM motion so that there is no leakage or loss of data during this migration

4. Termination of the source VM: After the Live migration is complete, all the data (main and derived) to be removed or secured adequately and corresponding access levels changed appropriately.

5. Should have ability to support parallel hosting of the service in both the Cloud Service Providers: Such a capability to support parallel hosting of the service in both the Cloud Service Providers is critical to

facilitate final gradual transition of the service from Old Cloud Service Provider to the New Cloud Service Provider. This would have various nuances for IAAS, PAAS and SAAS.

Question 13. What should be the roles and responsibilities in terms of security of (a) Cloud Service Provider (CSP); and (b) End users?

Idea Response:

The advantage of cloud computing to the data driven industries is significant, especially to the SME's. However, currently the standards available in the cloud industry are sparse or rather it suffices to mention that there is no single standard available. Thus, a minimum set of guidelines can be formed. However, care needs to be taken to ensure that such guidelines do not in any way hinder the adoption of cloud.
Various terms and conditions / roles and responsibilities have been already laid down in various laws like Information Technology Act, Companies Act 1956, and Copy Right Act and these will be applicable to Cloud service providers and also the customers of the Cloud service. The same may be continued with for the time being.

The Authority also needs to consider jurisdictional issues in this regard.

Question 14. The law of the user's country may restrict cross border transfer/disclosure of certain information. How can the client be protected in case the Cloud service provider moves data from one jurisdiction to another and a violation takes place? What disclosure guidelines need to be prescribed to avoid such incidents?

Idea Response:

The advantages of Availability and Business continuity come with the cloud models allowing data to be ported across multiple data centers. The location of the data centers of the provider does not matter if:

a. The service provider declares the location of data and consent from the customer is obtained
b. The customer is the sole owner of the data
c. The customer data is protected and no foreign country has the jurisdiction of data.

As rightly pointed out in the CP, when effective regulations restrict the movement of data across borders or force the data to remain within national borders due to absence of cross jurisdictional alignment, the

providers lose out on advantages such as improvements through scale offered by collating data in multiple Locations.

Thus any restrictions on movement of data and location of data would inherently limit the efficiency and efficacy of cloud services, and should not be imposed under law. If any specific Security provisions are required, then can always be discussed with service providers. However in case restrictions are to be imposed on security issues, then same should be equally applicable to all service providers (cloud as well as telecom service providers) such that business opportunities are available to all in fair manner.

Question 15. What polices, systems and processes are required to be defined for information governance framework in Cloud, from lawful interception point of view and particularly if it is hosted in a different country?

Idea Response:

We believe that the existing frameworks under Indian information technology and criminal law (including Mutual Legal Assistance Treaties – MLAT) are sufficient to address any requirements in relation to lawful interception. Thus, there seems no need for any additional regulation at this point in time.

As rightly pointed out in the Consultation Paper under clause 5.23, "*Unduly onerous requirements should be carefully scrutinized from a cost-benefit perspective. A cooperative effort from all the stakeholders including technology industry, users of cloud services, service providers, bandwidth/connectivity providers and government is necessary to determine core cloud practices in order to provide greater clarity and predictability for individuals, customers and cloud providers".* Internet offers plethora of opportunities and India needs development of applications for diverse geographies, and convergence of developed world applications into usable Indian flavor applications. Pre-mature and Over-Regulation would kill the development of this eco system, and should thus be avoided at all cost.

However, as a safeguard, adequate training and capacity development may be done so as to effectively enforce existing provisions of law. This will ensure lawful interceptions activities are carried out effectively while ensuring service providers are burdened with avoidable requirements.

Question 16. What shall be the scope of cloud computing services in law? What is your view on providing license or registration to Cloud service providers so as to subject them to the obligations thereunder? Please comment with justification.

Idea Response:

In India, as cloud services are at a very nascent stage, any restrictions in the form of licensing or registration may hamper expansion of these services. We thus feel that Cloud Service providers should be allowed to mushroom and no license / registration is needed at this stage.

Innovation should be encouraged and India should benefit from high quality IT specialists who want to turn cloud entrepreneurs. It is thus critical that their cost structure is kept low at this stage.

Internet offers plethora of opportunities and India needs development of applications for diverse geographies, and convergence of developed world applications into usable Indian flavor applications. All individuals, organizations including telcos and non-telcos should thus have the freedom to utilize the cloud services without any un-needed restrictions.

Thus, Cloud solutions should not require any separate licensing or registration requirements.

Question 17. What should be the protocol for cloud service providers to submit to the territorial jurisdiction of India for the purpose of lawful access of information? What should be the effective guidelines for and actions against those CSPs that are identified to be in possession of information related to the commission of a breach of National security of India?

Idea Response:

As already submitted by us, any Pre-mature and Over-Regulation is likely to negatively impact the development of cloud eco system, and should thus be avoided at all cost. National security and lawful access to information are legitimate policy concerns, but there already exist laws to deal with any infringements on those fronts.

Towards that end, we believe that the existing frameworks under Indian information technology and criminal law (including Mutual Legal Assistance Treaties – MLAT) are sufficient to address any requirements in relation to lawful access of information as well as commissions of breach of national security. Thus, there seems no need for any additional regulation in that area at this point in time.

Question 18. What are the steps that can be taken by the government for?

(a) Promoting cloud computing in e-governance projects.

(b) Promoting establishment of data centres in India.

(c) Encouraging business and private organizations utilize cloud services

(d) To boost Digital India and Smart Cities incentive using cloud.

Idea Response:

It is reiterated that the advantages of Availability and Business continuity can only come with the cloud models that allow for data to be ported across multiple data centers without restrictions such as cross-border data flows. Regulations that prohibit free data flows or prescribe a limited set of permissible cases are not future-proof, will stop the march of technology and have unintended consequences for innovation, investments and the quality of experience for the users of the services. It is thus critical that Innovation be encouraged through enabling policy measures to allow India to benefit from high quality IT specialists who want to turn cloud entrepreneurs.

Further, as already submitted, cloud services in India are at a very nascent stage, and hence any restrictions in the form of licensing or registration are likely to hamper the expansion of these services. There is an accelerated requirement to incubate innovation in the cloud infrastructure space in order to make India the next generation international powerhouse destination in the cloud services including e-Health, e-Education and e-Governance. We thus feel that in order to allow for cloud Services / data centers to mushroom, no license / registration should be mandated at this stage.

Further, as per us, some of the primary tasks that can be taken up by the Government of India to promote Cloud services for e-governance, organizations and smart city projects are as follows

1. **Availability of bandwidth.**

    a. Connectivity to all cities, villages and taluks is critical and needs to be achieved at the earliest.
    a. Towards that end, RoW issues also need to be addressed in addition to reaching out optical fiber cable from District to Block headquarters and Block headquarters to villages so as to fulfill the backhaul bandwidth requirement for the provision of broadband..
    b. The cost of the bandwidth has to be made affordable for the common man

2. **Availability of power**

    a. To enable large data centers to come up to host the cloud service, power is a major constraint.
    b. Power availability to be ensured in Tier2 and Tier3 cities
    c. The cost of power to be low enough to enable the lowest possible cloud service charges to the citizens of the country

3. **Road/Rail/Air Connectivity:**

    Road/ Rail/ Air connectivity to Tier2 and Tier 3 cities for data centers will facilitate cloud service providers setup world class data center facility

4. Appropriate tax holidays to SME's and organizations using the cloud services will promote usage of the cloud.

5. Regulations to be flexible to enable the cloud providers service the customers

6. Policy on compliance of standards and frameworks to be defined so as to facilitate customers for portability across the cloud providers.

7. Encourage Indian organizations to promote and establish the cloud services.

8. A facilitating and enabling legal and regulatory framework is required to support and facilitate cloud computing deployment.

Question 19. Should there be a dedicated cloud for government applications? To what extent should it support a multi-tenant environment and what should be the rules regulating such an environment?

Idea Response

Considering that the Government of India has already recognized the importance of cloud-based service-delivery platforms for establishing the foundation of Digital India, as it integrates smart devices and infrastructure and processes data from the large amount of scattered sources in real time, India's huge population and the associated database, and security of the voluminous information involved, it might be worthwhile to have a separate dedicated cloud for all Government applications.

Since the Governance services require accessibility by multiple users at any particular instant of time, it is necessary that the dedicated cloud should be able to support a multi-tenant environment for the access of such services on that cloud. By adopting Cloud computing, government agencies can create a central pool of shared resources including software and infrastructure, and the same can be allowed to be used on a non-discriminatory basis by all government agencies.

The database and access of the same should be brought under the purview of the IT Act 2000 of the India.

Question 20. What infrastructure challenges does India face towards development and deployment of state data centers in India? What should be the protocol for information sharing between states and between state and central?

Idea Response:

India faces a number of infrastructural challenges toward development of state data centers as already highlighted above. Key challenges are as follows:

1. **Availability of bandwidth.**
    a. Connectivity to all cities, villages and taluks is critical and needs to be achieved at the earliest.
    c. Towards that end, RoW issues also need to be addressed in addition to reaching out optical fiber cable from District to Block headquarters and Block headquarters to villages so as to fulfill the backhaul bandwidth requirement for the provision of broadband..
    d. The cost of the bandwidth has to be made affordable for the common man

2. **Availability of power**

    a. To enable large data centers to come up to host the cloud service, power is a major constraint.

    b. Power availability to be ensured in Tier2 and Tier3 cities

    c. The cost of power to be low enough to enable the lowest possible cloud service charges to the citizens of the country

3. **Road/Rail/Air Connectivity:**

    Road/ Rail/ Air connectivity to Tier2 and Tier 3 cities for data centers will facilitate cloud service providers setup world class data center facility

In addition, a number of compliance-related barriers that inhibit expansion of telecom infrastructure in the country need to be addressed through suitable policy amendments. For such bottlenecks, the government needs to adopt measures aimed at improving the ease of doing business through faster approvals, single window clearances, and uniform guidelines across different jurisdictions.

Question 21. What tax subsidies should be proposed to incentivise the promotion of Cloud Services in India? Give your comments with justification. What are the other incentives that can be given to private sector for the creation of data centres and cloud services platforms in India?

Idea Response:

Data centers incur one-time and recurring taxes that have a significant impact on long-term costs for any data center. The capital-intensive nature of a data center leads to relatively high sales taxes and property taxes. The Government policies should offer tax-incentives and duty refunds that will encourage existing service providers from other jurisdictions to set up their operations within India.

Additionally, other form of benefits such as subsidized electricity/water tariffs, financial incentives on adoption of renewable sources of energy can also be looked at.