RJIL/TRAI/2016-17/569
3rd September 2016

To,

Shri Asit Kadyan,
Advisor (QoS),
Telecom Regulatory Authority of India,
Mahanagar Doorsanchar Bhawan,
Jawaharlal Nehru Marg,
New Delhi - 110002

Subject: Comments on TRAI's Consultation Paper dated 10th June 2016 on 'Cloud Computing'.

Dear Sir,

Please find attached comments of Reliance Jio Infocomm Limited on the issues raised in the Consultation Paper dated 10th June 2016 on 'Cloud Computing'.

Thanking You,

Yours sincerely,
For **Reliance Jio Infocomm Limited,**

Kapoor Singh Guliani
Authorised Signatory

RELIANCE JIO INFOCOMM LIMITED ★

Encl.: As above.

RJIL's Response to TRAI's Consultation Paper on 'Cloud Computing'

Preamble

At the outset we would like to thank the Authority for coming out with a consultation on Cloud Computing as we feel that this is a move in the right direction and can help in accelerating the adoption of cloud services in India.

We firmly believe that cloud technology can play a pivotal role in making the vision of Digital India a reality by presenting new possibilities in e-governance, healthcare, education and financial inclusion, impacting a billion lives, securely and at lower cost. A world-class cloud infrastructure can help Indian companies, government and entrepreneurs to be able to enhance productivity and efficiency, thereby acting as a catalyst for India's overall economic growth. Further as the cloud adoption is anyways taking up in the developed world and can anytime accelerate in India this is an opportune time for the government to create an enabling policy framework which will not only provide impetus to the growth of cloud based services in India but also ensure that the growth happens in a systematic manner and as per the defined standards.

Worldwide, cloud technology is witnessing strong growth due to more and more organizations realizing the inherent benefits of the technology such as reduction in costs, increased speed to adoption and ability to transform business processes. The global public cloud services market is projected to grow 16.5 percent in 2016 to total $204 billion, up from $175 billion in 2015, according to Gartner, Inc. The highest growth is likely to come from cloud system infrastructure services (infrastructure as a service [IaaS]), which is projected to grow 38.4 percent in 2016, to reach $ 22.4 billion. Cloud application services (SaaS) is forecast to grow 20.3 percent in 2016, to $37.7 billion. As software vendors shift their business models from on-premises licensed software to public cloud-based offerings, this trend will continue.

The cloud market in India also has a fairly positive outlook. As per the '2016 ITA Cloud Computing Top Markets report' the total cloud spending is anticipated to reach almost **$2 billion** by the end of the decade. Indian **cloud data center traffic is likely to increase four-fold by 2017** with **17% of services accessed by mobile users,** according to the third annual Cisco Global Cloud Index. Adoption of cloud based services is also likely to make a significant contribution in the creation of IT Jobs in India. According to research firm International Data Corp. (IDC), cloud will provide **40% more IT Jobs** in India by 2018.

Despite optimistic predictions and a definite increase in the adoption of cloud based platforms for citizen centric services like banking, insurance, healthcare and governance in the last few years, India's roadmap for cloud adoption still faces a lot of challenges. A recent study highlights that despite increase in awareness of cloud services amongst organizations, most of the large Indian enterprises host less that 15 % of their ICT process on cloud.

RELIANCE JIO INFOCOMM LIMITED

Issues like data security & privacy, lack of inter-operability and loss of control continue to plague the demand for cloud services in India. In addition to these, other impediments such as insufficient broadband infrastructure, unreliable power supply across various parts of the country and lack of incentives for setting cloud data centers further add to the woes of the cloud industry.

Given the unique mix of opportunities and challenges posed by cloud computing, the government needs to play a pivotal role in ensuring that the Indian entities benefit from the cloud revolution without being encumbered by the risks and challenges that arise from cloud.

General Comments

1. **National Security and Data Hosting**:

   a. While there is great interest in cloud based solutions in India, general apprehensions remain about whether cloud services can ensure adequate protection of sensitive information for government departments and organizations. Protection of national interests, National security and apprehension over possible foreign surveillance, especially when most of the CSPs are foreign, are top prohibiting concerns vis-a-vis cloud services for the government sector.

   b. On the primary concern of ensuring that there is no breach of national security or sensitive information, it is critical that the government pushes for data hosting in India. The policy framework should ensure that the foreign firms involved in providing cloud services in India are mandated to host the India centric data in India only and no data is allowed to move outside India. The Indian government has been rightfully supporting the idea of foreign firms storing data in India. The recent policy initiatives by different wings of Government of India point to this direction, viz.

      i. The guidelines for "National Telecom M2M Roadmap" call for "all M2M gateways and application servers" used in providing services to individuals in India to be physically located within the country. Although, cloud vendors are not the main focus of this provision but this provision points to the acceptance and need of data localization policies in the Indian government.

      ii. Another push for data localization can be seen from DeiTY. As per the RFP for Provisional Accreditation of Cloud Service Offerings of Private Service Providers, providers are mandated to host data within India.

RELIANCE JIO INFOCOMM LIMITED ★

c. **Given that National security is the matter of utmost prominence for India, RJIL strongly advocates that any service provider offering cloud based services should be mandated to have data centers within India. This becomes even more relevant and important when it comes to storage of government data. We must ensure that under no circumstances the Indian data can move beyond India's geographical territories.**

2. **Interoperability:**

a. Interoperability is the key to the exponential growth of cloud computing. Vendor lock-in on account of lack of interoperability between various cloud platforms is one of the biggest fears and impediment for cloud users. Therefore ensuring higher interoperability will not only help in providing customers with greater choice but will also go a long way in fostering competition and innovation by allowing more players in the market.

b. **Open access/ open source policies that allow extension of APIs and specifications** should be supported by the policy makers to ensure that multiple cloud platforms can exchange information in a uniform manner and ultimately work together seamlessly.

c. To realize desired interoperability it is vital that there are well defined standards at all levels i.e. infrastructure, platform, application service, data and management. Understanding this critical need of standardization, many governments and consortiums have set out initiatives to foster cloud interoperability. Many international bodies like **Open Group, IEEE, ITU Focus group on cloud computing, NIST, China Electronic Standardization Institute** have done considerable amount of work in defining standards and reference architectures for cloud computing.

d. Conforming to the internationally accepted interoperability standards should be made a part of acceptable best practices for all existing and prospective cloud service providers. **However, given that cloud computing is at a nascent stage, any mandatory regulatory framework for inter-operability is likely to kill innovation and slow the industry growth at local level.**

3. **Security and privacy:**

a. The biggest challenge hindering the adoption of cloud computing is the risks it poses to the **security and privacy. Protecting data from theft and unauthorized access** is one of the most crucial requirements in a cloud environment especially during transit and in case of multi-tenant environments.

RELIANCE JIO INFOCOMM LIMITED

b. Encryption, is one of the widely used tools for protecting data and it should be a mandatory requirement for data in transit as well as at rest.

c. Apart from encryption, established practices for authentication and identity management should be adopted to ensure only the authorized users are allowed to access sensitive data and applications. Data masking is also a widely adopted technique aimed at reducing risk of exposing sensitive information.

d. Adoption of **international standards such as ISO 27000 series and Information Infrastructure Library (ITIL)** service management infrastructure best practices can help in reducing data security related vulnerabilities. However, imposing any kind of mandatory regulations is not recommended at this stage given that Indian cloud industry is still at a very nascent stage.

4. Government Support:

a. While there has been a growth in the number of data centers in India in the last few years, **India still lags behind both in number as well as sophistication of data centers** it hosts. It is important the government takes adequate measures to ensure that Indian service providers are incentivized to build best in class infrastructure for cloud. Some of the financial measures that can be adopted by the government in this regard can be :

   i. Allowing private Indian CSPs to procure raw infrastructure such as servers, firewalls etc at a subsidized rate for setting up cloud infrastructure.

   ii. Incentivize banks to extend loans at concessional rates for setting up cloud infrastructure.

   iii. Providing tax incentives or tax holidays to Indian CSPs for a defined period of time.

   iv. State governments to provide land at subsidized rates for setting up cloud data centers.

b. Apart from these financial provisions it is important that that the government takes specific measures which improve the ease of doing business for private cloud service providers. Facilitating a single window of clearance process for cloud data centers and creating a streamlined policy framework can go a long way in making India a hub of world class cloud data centers.

5. **Insufficient broadband infrastructure**

a. As acknowledged by the Authority, the broadband infrastructure in India is extremely insufficient and this coupled with major gaps in physical infrastructure

RELIANCE JIO INFOCOMM LIMITED

like inconsistent power supply across various parts of the country are some of the key deterrents for adoption of cloud based services.

b. According to the United Nations, India meets the minimum Internet infrastructure standards necessary for only basic cloud services, with bottlenecks impacting download speeds, upload speeds and network latency. Further, the World Economic Forum ranked India a dismal 113 out of 142 countries with the availability of international Internet bandwidth, a measure of the amount of Internet traffic that can be exchanged between countries.

c. We understand and appreciate that the Authority is focused on addressing the issues related to broadband infrastructure and it has initiated various policy initiatives on this, however, we are still a long way from addressing these inadequacies in infrastructure and hence the government should take immediate measures to improve the provision of reliable and affordable internet/broadband infrastructure.

d. **Bringing uniformity in ROW policy/rules across states and timely allocation of spectrum** are some of the immediate measures which the government should look at.

6. Well-defined cloud policy for Government departments

a. The Government should formulate guidelines for usage of cloud across various departments and functions in the government, post-haste. If the Government data is moved to the Cloud then this will be the single largest push towards adoption of cloud services, this will also generate a confidence in private sector to follow this path. Therefore a clear-cut and mandatory policy is absolutely essential to ensure wide scale adoption by various government entities. This can also play an important role in reducing the current inefficiencies in government's IT environment like low asset utilization, fragmented demand for resources, duplicative systems, environments which are difficult to manage and long procurement lead times.

b. There are international precedents for such a step. The US government has already taken a step towards a "Cloud First Policy" which now mandates the federal agencies to move to cloud-based solutions whenever a secure reliable and cost effective cloud option exists. On similar lines, the government of UK has also undertaken a government wide cloud strategy. The British Government's G-Cloud has a hybrid Cloud structure with a public-private architecture catering to multiple Cloud communities.

c. In line with its effort to increase cloud adoption, the US Government has also created the National Institute of Standards and Technology – a federal technology agency that works with industry to develop and apply technology, measurements, and standards to be used by industry as well as Government agencies.

d. Thus, a comprehensive policy framework should be put in place covering all aspects such as data protection requirements for classified government data, access controls & data controls, statutory compliance to laws, regulations and agency requirements, governance procedures, QoS requirements and DR mechanism.

e. Taking a cue from some of the above global initiatives, the Indian government is also working on creating a cloud policy as well as setting up of Cloud Management Office (CMO) which will be the central agency responsible for defining standards and guidelines for empanelment of CSPs. However, the government needs to accelerate the process and mandate moving to cloud in a time bound manner to ensure that there is no further delay in cloud adoption on account of lack of clarity in direction and guidelines for government as a user.

Keeping above in view, our response to the various questions raised in the consultation paper are provided seriatim in this paper.

Response to Questions:

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.

RJIL Response:

Cloud computing has impacted the way in which technology is delivered and consumed by organizations. Adopting cloud technology not only helps organizations in reducing total cost of ownership (TCO) but also provides them with the much needed flexibility and agility in today's dynamic environment.

As per EY's Enterprise IT Trends and investment survey (2014), one in every two Indian CIOs ranked cloud services and IT consolidation as their top investment priorities. This is primarily driven from the need of organizations/enterprises to reduce their IT infrastructure and administrative costs.

Some of the key cost benefits which accrue from moving to a cloud model are as follows:

i. **Shift from Capital expenditure (CapEx) to OpEx:** Cloud eliminates the capital expenditure completely. It represents a pay-as-you go approach to ICT, rather than an incremental capital expenditure approach. Initial expenditures are comparatively low and operating expenses go up or down depending on usage, so cash flow matches TCO.

RELIANCE JIO INFOCOMM LIMITED ★

ii. **Lower power costs:** Energy consumption adds a significant burden on the operating costs for organizations. In comparison to running own data centers where servers are typically under-utilized, cloud environment enables better utilization of hardware leading to more efficient use of power. In addition, while the operators of small data centers must pay the prevailing local rate for electricity, large providers can pay significantly lower rates by locating its data centers in locations with inexpensive electricity supply and through bulk purchase agreements.

iii. **Lower people costs:** Cloud computing significantly lowers labor costs as it does not require as much provisioning, software development, or maintenance as a conventional infrastructure due to automation of many repetitive tasks.

iv. **Measured services:** A cloud implementation can automatically control and optimize resources by metering services which makes it easier for managers to track expenses, establish charge-backs, and integrate cost controls into their future plans. Multiple payment models are possible, including pay for use, subscription, and fixed plans.

v. **Reduced Opportunity Cost:** Cloud computing frees the cash that can be used to invest in other parts of businesses and hence lowers the opportunity cost.

a) **Accelerating the design and roll out of services and b) promotion of social networking, participative governance and e-commerce c) Expansion of new services.**

As the pace of technology quickens, businesses are looking for IT solutions that enable them to react quickly, innovate smoothly and efficiently, and keep their growing pains to a minimum. Due to it's inherent benefits cloud computing can help firms in accelerating the design and roll out of services and also provide the much need flexibility and agility that is required for social networking, e-governance and e-commerce industry.

i. **Simple scalability:** With a cloud platform, managers can add capacity on demand without having to determine requirements beforehand or go through many of the traditional procurement, provisioning, and implementation processes. Load fluctuations are less of a problem when capacity can be added almost instantly.

ii. **Elastic services:** The cloud approach makes it easier for organizations to expand or contract services quickly by tapping into shared pools of resources or implementing pre-packaged capabilities developed by third parties specifically for clouds. Furthermore, private cloud deployments using multitenant servers mitigate the "server sprawl" that often accompanies growth.

iii. **Fast deployment:** With software vendors increasingly delivering their products preinstalled in virtual machines, much of the traditional installation and configuration work associated with software deployment may not be necessary for a cloud implementation leading to faster deployment.

iv. **Increased flexibility:** The variety of cloud deployment and service models ensures that implementations can be aligned closely with business needs and ICT strategies. Many public sector organizations are choosing a hybrid cloud approach that lets them benefit from both private and public clouds.

RELIANCE JIO INFOCOMM LIMITED

v. **Mobility:** Cloud computing allows its customers to access products and services from anywhere and anytime through mobile devices.

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?

RJIL Response:

The emergence of cloud services is fundamentally shifting the economics of IT. Cloud technology standardizes and pools IT resources and automates many of the maintenance tasks done manually today. Cloud architectures facilitate elastic consumption, self-service, and pay-as-you-go pricing.

As rightly pointed out in the consultation paper, cloud allows core IT infrastructure to be brought into large data centers that take advantage of significant economies of scale in three key areas:

i. Supply-side savings: Large-scale cloud data centers (DCs) lower costs per server. The economies of scale typically emanate from the following benefits :
   - o Lower cost of power for larger data center facilities: Power User Effectiveness (PUE) tends to be much lower in large facilities compared to smaller ones.
   - o Greater buying power: Operators of large data centers can get discounts on hardware purchases of up to 30 percent over smaller buyers.
   - o Reduced Infrastructure labor cost: While a single system administrator can service approximately 140 servers in a traditional enterprise, in a cloud data center the same administrator can service thousands of servers.

ii. Demand-side aggregation: Aggregating demand for computing smoothens overall variability, allowing server utilization rates to increase.

iii. Multi-tenancy efficiency: The virtualization of IT processes allows multiple clients to operate on the same physical network on a "multi-tenancy" basis. In a multitenant application model, increasing the number of tenants (i.e., customers or users) lowers the application management and server cost per tenant. This is benefit is accrued mainly due to amortization of fixed component of server utilization as well as fixed application labor over a large number of customers.

All the above factors lead to lower TCO (Total Cost of ownership) which in effects leads to lower IT budgets. According to study a 100,000 server Datacenter has 80% lower TCO compared to a 1000 server Datacenter.

Apart from the above benefits which accrue due the resource pooling capability of cloud computing, the scale of modern data centers also allows for economies of scale in terms of research, development, and reinvestment.

RELIANCE JIO INFOCOMM LIMITED ★

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?

RJIL Response:

As cloud computing is gaining adoption by organizations due to its immense benefits, the companies define their strategies based on their specific needs. The larger organisations can plan for customised cloud services, whereas the smaller ones have to choose the best fit from the available CSPs. There is no single defining strategy and nor a single cloud model that fits all organisations.

The cloud systems are generally operated in one of the three standard deployment models discussed below. However, there are subtle and major differences with each cloud model and the working of each model is unique.

Public cloud: In this model the ownership belongs to the service provider and there is no restriction on who can and cannot use the cloud. End users have the option of renting and adjusting resources based upon their own consumption pattern.

Private cloud is owned or rented by an organization for its private use.

Community cloud is similar to Private cloud but here resources are shared between members of a closed group who have the same needs.

Hybrid cloud is combination of two or more cloud infrastructures (which can be public, private or community) /provide extra resources in cases of high demand.

Organizations planning to move to cloud technology generally compare these models on the on parameters like tenancy, level of security, level of virtualization etc. and decide their best fit. We are providing a comparison of the various cloud deployment models on the possible parameters, that can help an organisation decide on its choice of model.

	Public Cloud	**Private Cloud**	**Hybrid Cloud**
Level of Abstraction	High	Low	Moderate
Tenancy	Either a single-tenant (dedicated) or multi-tenant (shared) operating environment	Single-tenant (dedicated) operating environment	A combination of public and private cloud offerings that allow for transitive information exchange
Level of Security	Low. No access to data in provider premise	High. Full access to data is available	High. Full access to data is available
Vendor Lock-in chances	Depends upon the technology that the vendor uses	High. Depends upon the technology used by provider.	Depends upon the technology used by the vendor
Capital Expenditure	Low. As most of the infrastructure is maintained by the provider	High. The in-house infrastructure has to be prepared for deployment	High

RELIANCE JIO INFOCOMM LIMITED

Operational Expenditure	High. Continuous pay per usage charging	Moderate. Only one time setup charge is high	Moderate
Managed by:	Third party	Organization or third party	Both Organization and Third party
Suitable for :	SMB, startups	Enterprise	Both
Data Privacy	Low	High	Moderate
Legal and compliant issues	High since data may have to be stored on foreign land	Low since data resides in our own data center	Low since data resides in our own data center
Types of application Suitable	Less mission critical application having less integration level	Application dealing with highly confidential data	Application dealing with highly confidential data
Infrastructure Owned by:	Third party	Organization or third party	Both Organization and Third party

Source: Infosys; Cloud Computing: Vendors Selection parameters and Comparison of Deployment Model.

In terms of selection of cloud model, there is no one-size-fits-all approach. Businesses should consider working with a technology partner who has adequate domain expertise to understand their industry specific requirements, regulatory needs and competitive pressures to architect cloud infrastructure. Some of the aspects that businesses need to consider before selection of the cloud model are:

- What is the current state of business and how well it operates today?
- Where are the efficiencies, gaps, risks, and opportunities for change?
- What is the plan to manage change and achieve the intended ROI?

For a smaller or medium size enterprises cost optimization maybe the most important factors while selecting the cloud model. Whereas for larger enterprises factors like operational efficiency and data security gain more importance.

Thus, when a company is considering a cloud deployment model for improving business outcomes it should consider how the cloud can fit into its business strategy and needs.

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

RJIL Response:

Migrating from one cloud to another is a complex process that requires careful planning and deliberation. There are many cloud migration issues, such as unexpected costs, interoperability, security gaps and unanticipated application rework that needs to be considered. In addition, when organization is migrating from one cloud to another, it's important to understand the process and temper any exorbitant expectations.

Inter Cloud Migration and Deployment needs strategy to resolve the complications that are involved in migrating various elements. For every migration broadly there are three categories in which these migrations can be categorized

RELIANCE JIO INFOCOMM LIMITED

- Migration to IAAS (Infrastructure as a Service) – requires planning of Dynamic Resource requirements, Storage requirement, Special H/W devices requirements, Volume of Data in/out
- Migration to PAAS (Platform as a Service) – requires analysis of Programming Language used, Databases, Middleware, Third Party Libraries and Restrictions of PAAS
- Migration to SAAS (Software as a Service) – Needs review of Architecture

A carefully carved out strategy in all these areas ensures that the migration is successful.

Adopting some of the best practices models provided by **ITIL** and the **ISO 27000** series can provide a good framework for structuring migration or transition.

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?

RJIL Response:

As mentioned in the earlier sections, having adequate control over data is one of the most crucial requirements in a cloud environment especially during transit. Essentially the regulatory provisions shall address all the possible concerns on this aspect.

The questions relating to data for cloud computing are about following forms of risk:

✓ **risk of theft or unauthorized disclosure of data,**
✓ **risk of tampering or unauthorized modification of data,**
✓ **risk of loss or of unavailability of data.**

Security considerations apply both to data at rest (held on some form of storage system) and also to data in motion (being transferred over some form of communication link). Encryption of data-in-transit and data-at-rest should be mandated in a cloud environment to reduce security related risks.

a) For securing data in motion CSPs should be mandated to support one or more of the following security standards :
   ✓ HTTPS - for regular connections from cloud service customers over the internet to cloud services
   ✓ SFTP - for bulk data transfers
   ✓ VPN using IPSec or SSL - preferable for connections from employees of the customer to the cloud service

b) For data at rest (*data stored within a cloud service*) – the CSPs should ensure that all sensitive data is encrypted.

   There can be multiple architectural approaches for encryption in cloud computing – storage device level, agent based, file system based and application level.

   ✓ Client/Application Encryption: Data is encrypted on the endpoint or server before being sent across the network or is already stored in a suitable encrypted format. This includes local client (agent-based) encryption (e.g., for stored files) or encryption integrated in applications.

- ✓ Link/Network Encryption. Standard network encryption techniques including SSL, VPNs, and SSH. Can be hardware or software. End to end is preferable but may not be viable in all architectures.
- ✓ Proxy-Based Encryption: Data is transmitted to a proxy appliance or server, which encrypts before sending further on the network. Often a preferred option for integrating into legacy applications but is not generally recommended.

Apart from encryption, data masking is also a widely adopted technique aimed at reducing risk of exposing sensitive information. This can also be made a part of regulatory provisions. Insisting that cloud service providers comply to **well-established security standards and industry certifications** such as ISO 27001, PCI DSS, FIPS 140-2 etc can go a long way in keeping the data security threats at minimal.

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?

RJIL Response:

Interoperability is the key to the exponential growth of cloud computing. Vendor lock-in on account of lack of interoperability between various cloud platforms is one of the biggest fears for cloud users. Ensuring higher interoperability can not only help in providing customers with greater choice but go a long way in fostering competition and innovation by allowing more players in the market.

As rightly explained by TRAI, some of the approaches that can be adopted to ensure greater levels of inter-operability in a cloud environment are:

1. Development of a common or unified cloud computing interface to facilitate a decentralized, extensible and secure hybrid computing environment.
2. Creation of a unified orchestration layer to support a multi- vendor environment
3. Adoption of Open Cloud Computing Interface (OCCI) model by Open Grid which is a protocol and API for all management tasks.

Apart from this, pushing for **Open access/ open source policies that allow extension of APIs and specifications** is extremely important to ensure that multiple cloud platforms can exchange information in a uniform manner and ultimately work together seamlessly.

To realize desired interoperability it is also vital that there are well defined standards at all levels i.e infrastructure, platform, application service, data and management. Understanding this critical need of standardization, many governments and consortiums have set out initiatives to foster cloud interoperability. **Open Group, IEEE, ITU Focus group on cloud computing, NIST, China Electronic Standardization Institute, DMTF** are some of the global bodies who have done considerable amount of work in defining standards and reference architectures for cloud computing. (*refer appendix for more details*)

RELIANCE JIO INFOCOMM LIMITED

The Indian government should also work closely with these global organizations who are working towards standardization and put in dedicated efforts in setting these standards.

Customers of cloud services must insist that their cloud providers adopt or align to these global standards and best practices to ensure greater degree of inter-operability.

However, given that cloud computing is at a nascent stage, any mandatory regulatory framework for inter-operability is likely to kill innovation and slow the industry growth at local level.

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.

RJIL Response:

With the rapid development of cloud computing, more and more cloud service providers are joining cloud market giving businesses and consumers more choice. However, comparing the service offerings between cloud service providers and assessing their performance is not a straightforward exercise.
Some of the metrics which can be considered for measuring performance and effectiveness of cloud service providers for different services are as follows:

✓ **Availability**: Availability is the proportion of time a system in functioning condition. For cloud service availability, it can be defined as the capacity of an IT system to provide continuous service delivery. For e.g., a 99.9% SLA (service-level agreement), in practice, means that in any given month (assuming a 30-day month), the service can only be unavailable for about 4 minutes and a few seconds, or only about 50 minutes per year.

✓ **Reliability**: Refers to the ability to ensure a continuous process of the program without loss.

✓ **Scalability**: For cloud service, scalability is the ability of the whole system to sustain increasing workloads by making use of additional resources.

✓ **Elasticity**: Elasticity has become a key metric of cloud service. It is an ability of a system to adapt to change in workloads and resource demands.

✓ **Security**: Cloud service concerns a number of security issues, such as software platform security and infrastructure security via the cloud.

✓ **Service capability**: Service capability is the degree of capability in a service system to provide services and is commonly defined as the maximum output rate of the system.

Below is the summary of essential parameters:-

Service-level category	**KPIs**	**Definition**	**Unit of Measurement**
Availability	Service window	Time window within which KPIs are measured	Time range

RELIANCE JIO INFOCOMM LIMITED ★

	Service/System availability	Percentage of time that service or system is available	%
	MTBF	Meantime between failure	Time units
	MTTR	Meantime to repair	Time units
Performance	Response time	Response time for composite or atomic service	Seconds
	Elapsed time	Completion time for a batch or background task	Time units
	Throughput	Number of transactions or requests processed per specified unit of time	Transaction or request count
Capacity	Bandwidth	Bandwidth of the connection that supports a service	Bps
	Processor speed	Clock speed of a processor	MHz
	Storage capacity	Capacity of a temporary or persistent storage medium, such as RAM, SAN, disk, or tape	GBx
Reliability	Service/System reliability	Probability that service or system is working flawlessly over time	%
Scalability	Service/System reliability	Degree to which the service or system can support a defined growth scenario	Yes/No, or description of scalability upper limit

All these metrics for measuring performance and effectiveness of cloud services should be established prior to subscribing to cloud services and should be specified in the cloud SLAs at the time of contracting.

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?

RJIL Response:

Cloud is utility based computing system. We pay for it in a similar manner as we pay for utilities like electricity, water and gas. These utilities are measured by number of units

RELIANCE JIO INFOCOMM LIMITED

consumed. But in cloud no proper way is established which shows that we have been charged for the same, that we utilized. Hence, consumers are invariably bogged down by concerns over accuracy of their bills in a cloud environment.

In such a scenario the accounting of resources used and billed needs to be sustained by the cloud service provider. Some of the steps that can be adopted by CSPs are:-

- Preserving the complete logs and all such other details which are essential for the complete satisfaction of the client. The satisfaction of the client with the billing performance can be assured by :
    - ✓ Timely generation of the bill,
    - ✓ Accuracy and completeness of the bill,
    - ✓ Clarity in bills/ presentation of the billing information in terms of transparency and understandability, and
    - ✓ An established and transparent process for resolution of billing complaints.

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

RJIL Response:

It is imperative that consumer complaints and public grievances are resolved in a timely, efficient and cost-effective manner through a system that is easily available all across the country.

Cloud service provider must design and provide a well-structured multilayered Customer Grievances Redressal Mechanism including Customer Dispute Resolution Mechanism. Customers having complaints or grievances should be able to interact with the organization/ register its grievances through 24X7 telephonic chat and web support, IVR to call center, e-mail or through web portal. Raised complaints must be addressed as soon as possible. Record of all the details such as raised tickets, open tickets, on-going tickets, closed tickets, time taken in resolved tickets should be maintained.

The consumer grievance redressal mechanism and associated analysis in telecom services can be a good reference point for mandating the consumer grievance redressal mechanism for TSPs.

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

RJIL Response:

As customers transition their applications and data to use cloud computing, it is critically important that the level of security provided in the cloud environment is equal to or better than the security provided by their traditional IT environment.

RELIANCE JIO INFOCOMM LIMITED

The Clouds Standard Customer Council (CSCC) prescribes a series of ten steps that cloud service customers should take to evaluate and manage the security of their cloud environment with the goal of mitigating risk and delivering an appropriate level of support.

i) **Ensure effective governance, risk and compliance processes exist** :
Adopting well defined practices for governance, risk & compliance in a cloud environment, ensure that all the systems and processes are implemented and used according to agreed-upon policies and procedures. This in turn minimizes the threats on account of unpredictability in a complex cloud environment.

It is recommended to ensure compliance to some of the generic IT governance standards like **COBIT, ITIL, ISO 20000 series of standards, SSAE16, ISO 38500** etc to ascertain that all assets within the cloud environment are properly controlled and maintained.

In addition to these general standards and frameworks, cloud customers can also insist on specific standards which operate at country or regional levels or which apply to specific industries or to specific types of data. E.g HIPAA, PCI DSS, FedRAMP, FISMA etc.
There are also some standards like ISO/IEC 27000 series that deal specifically with governance and management of information security, including the identification of risks and the implementation of security controls to address these risks.

ii) **Audit operational and business processes:** Customers must ensure that the cloud service provider is open to third party audits to so that the security gaps and risks in a cloud environment can be assessed. The auditors must be able to audit current controls and also access audit trails in the form of historic log data for the systems used to provide cloud services. This can go a long way in providing consumers with additional assurance.

iii) **Manage people, roles and identities:** Established practices for authentication and identity management should be adopted to ensure only the authorized users are allowed to access sensitive data and applications.

For people performing roles for the customer, in particular users and administrators of cloud services, it is necessary to have suitable **Identity & Access Management (IAM)** in place to ensure that a person must identify and authenticate themselves when using the cloud service and that they are granted access rights which are appropriate to their role.

Cloud computing customers should look for IAM capabilities that support:

- ✓ **Federated IDs**
- ✓ **Single sign-on**
- ✓ **Privileged Identity Management**
- ✓ **Multi-factor Authentication**

RELIANCE JIO INFOCOMM LIMITED

Cloud customers should insist for standards and technologies which provide federated IDs and single sign-on, such as LDAP, SAML 2.0, SCIM etc to ensure appropriate and controlled access to customer data and applications in the cloud computing environment.

iv) **Ensure proper protection of data and information**: Security considerations apply both to data at rest (held on some form of storage system) and also to data in motion (being transferred over some form of communication link). Encryption of data-in-transit and data-at-rest should be mandated in a cloud environment to reduce security related risks.

a) For securing data in motion CSPs should be mandated to support one or more of the following security standards :
   - ✓ HTTPS - for regular connections from cloud service customers over the internet to cloud services
   - ✓ SFTP - for bulk data transfers
   - ✓ VPN using IPSec or SSL - preferable for connections from employees of the customer to the cloud service

b) For data at rest (*data stored within a cloud service*) – the CSPs should ensure that all sensitive data is encrypted.

As mentioned in the response to question 4, multiple encryption techniques/approaches can be adopted to reduce data security threats. Apart from encryption, data masking is also a widely adopted technique aimed at reducing risk of exposing sensitive information.

Customers should insist that cloud service providers comply to **well-established security standards and industry certifications** such as ISO 27001, PCI DSS, FIPS 140-2 etc. This can go a long way in keeping the data security threats at minimal.

v) Enforce privacy policies

Privacy primarily relates to the acquisition, storage and use of **personally identifiable information (PII)**. Any cloud service customer must give serious consideration to any PII that they intend to store or process within a cloud service.
It is important that privacy related issues are dealt with in the cloud service contract and service level agreement.

There are some specifications and standards which relate to privacy and the handling of PII. One of the established frameworks is the U.S – EU Safe Harbor framework, which enables US based companies to certify their compliance to the requirements of the EU data protection directives. This is further supported by commercial certification offerings, such as the TRUSTe Safe Harbor certification seal program. Cloud service customers can use this framework as an assurance that a cloud service provider is treating PII in an appropriate fashion.

RELIANCE JIO INFOCOMM LIMITED ★

vi) **Assess the security provisions for cloud applications**: Organizations must apply the same diligence to application security as they do for physical and infrastructure security.

In order to protect an application from various types of threat, it is typical to define a set of policies which apply to the deployment and provisioning of the application.

For cloud computing, it is important to understand the application security policy implications of the different cloud service models. The type of cloud service is very likely to affect the key question of who is responsible for handling particular security controls. For IaaS, more responsibility is likely to be with the customer (e.g. for encrypting data stored on a cloud storage device); for SaaS, more responsibility is likely to be with the provider, since both the stored data and the application code is not directly visible to or controllable by the customer.

Some of the technologies and techniques that can be considered in relation to cloud applications are:

- ✓ Firewalls to control access to applications and systems.
- ✓ VPNs to limit access to applications to users with authorization to access the VPN.
- ✓ Denial-of-Service countermeasures for any service endpoints that are exposed publicly on the internet.
- ✓ Countermeasures for the OWASP Top 10 application vulnerabilities should be considered

Adhering to NIST's Guidelines on Firewalls and Firewall Policy, can also help in mitigating threats related to application security in cloud environment.

vii) Ensure cloud networks and connections are secure

A cloud service provider must ensure that it allows only legitimate network traffic and drops any malicious network traffic. Consumers should expect a certain amount of external network perimeter and internal network separation measures from their cloud service providers.

In order to ensure that the cloud networks and connections are secure, the cloud customers should insist on certifications like ISO 27002 which provide detailed guidance on implementing network security controls.

Even if a cloud service provider has no network security attestation or certification, customers should at least ensure that a cloud service provider has documented and tested processes for:

- ✓ Access controls, for management of the network infrastructure
- ✓ Traffic filtering, provided by firewalls
- ✓ Creating secure Virtual Private Networks (if VPN is offered)
- ✓ Intrusion detection / prevention
- ✓ Mitigating the effects of DDoS attacks
- ✓ Logging and notification, so that systematic attacks can be reviewed

RELIANCE JIO INFOCOMM LIMITED ★

viii) **Evaluate security controls on physical infrastructure and facilities :**

An important consideration for security of any IT system concerns the security of physical infrastructure and facilities. Some of the measures that need to be taken to ensure safety of physical infrastructure/ data centers are as follows:

- ✓ All areas within the data center need to be monitored 24x7x365 by closed-circuit cameras and on-site guards.
- ✓ Data center space should be physically isolated and accessible only by authorized administrators.
- ✓ Access should be restricted to authorized personnel by two-factor biometric authentication.
- ✓ The provider should have appropriate backup of data, redundancy of equipment and continuity plans for handling equipment failure situations.
- ✓ Ensure CSPs to comply with recognized data center standards like TIA-942 which describe the requirements for the data center infrastructure in a thorough, quantifiable manner under four levels (called tiers) of data centers.

ix) **Manage security terms in the cloud SLA**

Given that cloud computing typically involves two organizations - the cloud service customer and the cloud service provider, security responsibilities of each party must be made clear. This is typically done by means of a service level agreement (SLA) which applies to the services provided, and the terms of the service contract between the customer and the provider.

Metrics for measuring performance and effectiveness of information security management should be established prior to subscribing to cloud services and should be specified in the cloud SLA. At a minimum, organizations should understand and document their current metrics and how they will change when operations make use of cloud computing and where a provider may use different (potentially incompatible) metrics.

The **European Network and Information Security Agency (ENISA)** has created guidelines for monitoring of security service levels in cloud contracts. As per the guidelines the specific metrics that should covered in contract include: **service availability, incident response, service elasticity and load tolerance, data life-cycle management, technical compliance and vulnerability management, change management, data isolation, and log management** & **forensics.** While this is not a standard, customers can leverage these guidelines to enhance their security levels through well-defined SLAs.

x) **Understand the security requirements of the exit process**

As highlighted in the response to question 11, the exit process or termination of the use of a cloud service by a customer requires careful consideration from an information security perspective.

To ensure cloud services are secure it is important to consider the above aspects, as failure to ensure appropriate security measures could ultimately result in higher costs and potential loss of business thus eliminating any of the potential benefits of cloud computing.

RELIANCE JIO INFOCOMM LIMITED ★

While CSPs should try and adopt international standards and best practices for security as mentioned in the above sections, imposing any kind of mandatory regulations is not recommended at this stage given that Indian cloud industry is still at a very nascent stage.

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

RJIL Response:

The exit process or termination of the use of a cloud service by a customer requires careful consideration from an information security perspective.

From a security perspective, it is important that once the customer has completed the termination process, "reversibility" or "the right to be forgotten" is achieved - i.e. none of the customer's data should remain with the provider. The provider must **ensure that any copies of the data are wiped clean from the provider's environment,** wherever they may have been stored (i.e. including backup locations as well as online data stores).

The exit process must allow the customer to **retrieve their data in a suitably secure form,** backups must be retained for agreed periods before being eliminated and associated event logs and reporting data must also be retained until the exit process is complete. At the end of the exit process, it is good practice for the provider to provide the customer with written confirmation that the process is complete and that the customers' data has been removed from the provider's systems.

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

RJIL Response:

Live migration allows flexible transfer of virtual machine from one physical server to another physical server without obstructing the services running in virtual machine. Secure live migration mainly aims to protect the VM from third party attacks during the migration process.

Following security provisions can be adopted for securing live migrations in a cloud environment:

i) **Isolating Migration Network**
In this approach the Virtual LAN consisting of the source and the destination host is isolated from migration traffic from other Network. This will reduce the risk of exposure of migration to the whole network.

ii) **Network Security Engine Hypervisor (NSE-H)**
This functionality provides extension to the hypervisor by providing functionality of firewall and IDS/IPS which secure the migration from external attack and can also detect

RELIANCE JIO INFOCOMM LIMITED

the network for the intrusion and hence an alarm can be generated in case of any intrusion detection.

iii) Secure VM-vTPM Migration protocols

Secure VM-vTPM migration protocol consists of various steps starting from authentication, attestation and data transfer stage. Firstly both the parties that is source VM and Destination VM authenticate each other for further communication. In the next step the integrity of the source and the destination is checked, only after verifying the integrity, the source VM start transfer to the destination VM. The file send by the source VM is stopped at the vTPM which encrypts the file and transfers to the destination VM. After completion of the transfer the file at the vTPM is deleted.

iv) Improved vTPM Migration protocol

This protocol is improved version of vTPM. It consists of trusted channel establishment and data transfer. The source VM and destination VM first authenticate each other to establish the trusted channel and then integrity verification is done. Both the source and the destination negotiate keys with each other using DH key exchange algorithm. After the channel is established VM and vTPM starts the transfer as usual.

v) Using SSH Tunnel

SSH tunnel is established between the proxies for secure migration. The proxy server at the source and the destination cloud communicate with each other and hides the details of the source VM and the destination VM.

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

RJIL Response:

Since cloud computing typically involves two organizations - the cloud service customer and the cloud service provider, security responsibilities of each party must be made clear.

Some of the responsibilities that the cloud service provider needs to undertake are:

i. Maintaining customer confidentiality and privacy.
ii. Providing adequate security controls and measures like encryption, data masking, auditing, logging, disaster recovery to protect and safeguard customer data.
iii. Ensuring availability of cloud services
iv. Adhering to leading global practices and international standards for ensuring security of cloud services.
v. Providing mechanism for monitoring and tracking performance and QOS parameters.
vi. Ensuring highest level of transparency in billing cloud customers.
vii. Providing the end users with notifications and the choice to change the business processes. Changes include upgrading a software-as-a-service application, introducing new versions of services, changing the location from which the service is provided, entering or exiting a business and closing a facility.

Some of the key **responsibilities of end user** that will in turn help both providers and consumers establish and maintain successful business relationships are:

RELIANCE JIO INFOCOMM LIMITED ★

i. Ensuring that contract with the cloud provider has appropriate security and privacy provisions and addresses liabilities, remediation and business outcomes.
ii. Retaining ownership of, and rights to use, their own data.
iii. Evaluating the external and internal network controls of the cloud service providers with respect to their requirements.
iv. Gaining clear understanding of the potential benefits and risks associated with security of cloud platform and the security processes the provider follows.
v. Understanding the legal jurisdictions, technical limitations or requirements of the services provided by CSP.

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?

RJIL Response:

This issue will be nonexistent in case the Cloud service providers are mandated to Host in India and it is ensured that no Indian data is allowed to go outside India.

However, in case the cloud services are being hosted in a different country, then it shall be mandatory for the Cloud service provider have full disclosure on the hosting aspect. This disclosure shall include:

a. Informing the customer beforehand the location of the data centre and the location of the disaster recovery site.
b. Providing a detailed information to the customer on the laws applicable on the data stored.
c. Clear and unambiguous information to the customers before movement of data planned by the Cloud service provider. This information shall include the details of applicable laws at new hosting location.
d. Providing the option of alternate location or sufficient time to move data to another CSP.

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?

RJIL Response:

As mentioned in the general comments section, **RJIL strongly advocates that any service provider offering cloud based services should be mandated to host data within India and under no circumstance shall the data move out of India.** This is extremely important as any sensitive data residing outside India can have serious implications on national security of the country.

RELIANCE JIO INFOCOMM LIMITED ★

Lack of control over physical information stored outside the jurisdiction limits the control which law enforcement agencies can wield over foreign players. This poses severe challenges in obtaining and analyzing data and log files from servers located outside India as they fall outside our jurisdiction.

National security and apprehension over foreign surveillance are top concern areas for the government. We are happy that the government is taking cognizance of these issues and trying to come out with right policies and framework for addressing them. To ensure that there is no breach of national security or sensitive information, Indian government has been rightfully supporting the idea of foreign firms storing data in India.

The benefits offered by local data storage are also aptly illustrated by the advantages the United States security apparatus enjoys due to the presence of so many data centers and the broad powers conferred on the federal government by the PATRIOT Act.

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.

RJIL Response:

The broad scope of cloud computing services in law should cover the following aspects:-

i. **Geo location of data storage and processing:** The geo-location of data storage and processing has important implications for end-user security as well data sovereignty and jurisdiction and hence should be included within the scope of legal framework.
ii. **Ownership of data:** The scope should include data subject rights relating to possession, custody and control of data
iii. **Data retention and deletion** is one of the important factor that should be included in the scope.
iv. **Information requests:** As cloud computing involves frequent transmission of data, the scope of law should also cover information requests.
v. **Security measures and backups:** The description of security and organizational measures to protect stored data should be part of the law.
vi. **Liability and warranties** should be included in the scope as it is critical for the customer because the main purpose of using cloud solution is the processing or storing of customer's data.

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?

RELIANCE JIO INFOCOMM LIMITED ★

RJIL Response:

The Cloud service providers may be brought under light touch licensing/registering regime in the beginning, in order to bring these under the umbrella of lawful security establishment.

The registration shall entail that the service provider will mandatorily provide information to the law enforcement authorities authorized to access information.

The authorization to access the information can be modelled on the lines of permission for lawful interception to avoid the misuse.

The government may impose strict 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. The registration of CSPs shall ensure that no CSP, not cooperating on such issues is allowed to offer cloud services in India.

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 centers in India.**
c) **Encouraging business and private organizations utilize cloud services**
d) **To boost digital India and smart cities incentive using cloud.**

RJIL Response:

Cloud computing offers an accelerator approach for economic growth due to its ability to connect people to data, information and computing resources anywhere and anytime. Cloud can drive the inclusive growth agenda by providing platform to scale the reach of education, healthcare, financial services, entrepreneurship and governance among other areas.

Indian Government has already started leveraging Cloud for the benefit masses and has launched massive projects like Aadhar, National Population Register, National Rural Heath Mission, M-NREGA on cloud based model.

Government's GI cloud initiative (*also referred as MeghRaj*) is the step in the right direction. The GI Cloud facility aims to ensure optimum utilization of the infrastructure and speeden up the development and deployment of e-Governance applications.

a) **Promoting cloud computing in e-governance projects and d) to boost digital India and Smart cities incentive using cloud**

Programs like Digital India, Smart cities and e-governance projects can immensely benefit from cloud technology provided the government takes the steps in the right direction. Some of the immediate measures that the government should take for promotion of cloud services are:

i. Formulation of cloud policy to lay foundation for large scale adoption of cloud in various government agencies.
ii. Incentivizing every central and state government department for adopting the cloud services will help in promoting the use of cloud based services like Digital Locker and providing a well-defined roadmap for adoption of cloud services.

iii. Creation of a nodal agency for laying standards and baselines for cloud adoption.

iv. Focusing on Skill enhancement and digital literacy programs.

v. Launching projects specific to industries like healthcare, education etc. on a cloud model.

vi. Encouraging PPP (public-private-partnership) model can help government in leveraging existing know-how and expertise of private sector.

vii. Drafting of technology-neutral standards for issues such as security and privacy, which can be flexible and allow government regulators to control the effects of technology without its implementation, leaving businesses with the challenge to innovate within that framework.

Countries like US and UK have initiated policies like Cloud First Policy (USA), Integrated Strategy (EU), G-Cloud Strategy (UK), Strategic Direction Paper (Australia) and Smart Cloud Strategy (Japan) to promote adoption of cloud in the government. Common features of these government initiatives include driving *cloud adoption, friendly legal framework, and devising a technology and international collaboration strategy.*

b) Promoting establishment of data centers in India

The data center industry is primarily driven by the kind of policy frameworks that governments prepare. Hence, a conducive framework that addresses the needs of data center industry with transparency, certainty and assurance is necessary.

It is important the government takes adequate measures to ensure that Indian service providers are incentivized to build best in class infrastructure for cloud. Some of the financial measures that can be adopted by the government in this regard can be:

- Allowing private Indian CSPs to procure raw infrastructure such as servers, firewalls etc at a subsidized rate for setting up cloud infrastructure.
- Incentivize banks to extend loans at concessional rates for setting up cloud infrastructure.
- Providing tax and duty incentives or tax holidays to Indian CSPs for a defined period of time.
- State governments to provide land at subsidized rates for setting up cloud data centers.

Apart from these financial provisions it is important that that the government takes specific measures which improve the ease of doing business for private cloud service providers. Facilitating a single window of clearance process for cloud data centers and creating a streamlined policy framework can go a long way in making India a hub of world class cloud data centers.

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?

RELIANCE JIO INFOCOMM LIMITED ★

RJIL Response:

Government of India has already envisaged empanelling cloud service providers and utilizing the capacity being built by them as part of GI Cloud initiative for providing services to the government departments.

Considering the data classification and security requirements, a dedicated government cloud infrastructure is suggested.

The infrastructure elements like server, storage (including backup storage) and network of the Government Cloud should provide strong tenant isolation, provide granular identity and access management capability and encryption and be logically separate from the public and other cloud offerings of the cloud service provider.

Government related data should not be hosted in any other country and there must be a clause to ensure that Government related data always stays inside India. It is also recommended that preferences should be given to Made in India Cloud service providers to host government specific requirements.

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

RJIL Response:

India faces a number of infrastructural challenges which hinder the development and deployment of state data centers such as **lack of reliable power supply**, **availability of adequate water infrastructure**, **pressures on land availability**, and **insufficient road infrastructure** in various parts of the country. Difficulties in obtaining **clearances and permissions** further adds to the woes of providers who are looking to set-up data centers in India.

In addition to the above inadequacies, India's **insufficient broadband infrastructure** (i.e constraints related to bandwidth and availability of fiber) is another key deterrent for proliferation of data centers in India. Lack of uniformity in ROW policies across states and delays in timely allocation of spectrum are the main reasons for the poor telecom infrastructure.

Addressing these inadequacies in infrastructure should be the top priority for the government. Some immediate steps like creating a single window of clearance for data centers, bringing uniformity in ROW rules across states, improving basic utility infrastructure and creating an enabling policy framework can go a long way in reducing these infrastructural challenges.

RELIANCE JIO INFOCOMM LIMITED ★

Question 21. What tax subsidies should be proposed to incentivize 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 centers and cloud services platforms in India?

RJIL 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 centre attracts relatively high sales taxes and property taxes. Further, electricity tariff, stamp duty charges, import duties on equipment sourced from outside India and multi-jurisdiction tax implications further impact data centre costing.

In the US, many states have passed legislation to provide customized incentives for data centres. These states provide full or partial exemption taxes for various investment types. The exemptions commonly cover computer (or IT) equipment across the board. Construction, mechanical and electrical equipment, cooling systems, power infrastructure, electricity, and backup fuel are all covered to varying degrees by this group of states.

In Singapore through the inclusion of related costs under the Productivity and Innovation Credit (PIC) scheme, cloud service providers are able to obtain significant tax benefits for cloud computing. Singaporean businesses, including small- and medium sized enterprises, can claim for their cloud computing expenditure, within certain categories such as the acquisition or leasing of technological equipment, training expenditure, the acquisition and registration of intellectual property rights, actual costs of research and development, and costs incurred in the creation of new products and industrial designs. The Info-communications Development Authority (IDA) of Singapore has been offering subsidies in the range of 50 to 100 percent to boost industry participation in Cloud.

In some other countries, cloud services are often provided via a network of local data centres, where they offer constantly changing special tax and other cash incentives. Some countries offer abatements or holidays for sales tax or Value Added Tax (VAT) or even reduced rates of overall income taxation based on profits derived from such cloud computing activities.

A proper structured framework is required to be devised and put in place for promoting cloud computing and to take advantage of India's leveraged position. A proper legal and regulatory framework and favourable tax structure is also required to support and facilitate cloud computing deployment.

Below are **some of the steps the government can take in this direction:**

- ✓ Data center and cloud companies should be declared under a special infrastructure category of national importance
- ✓ India can adopt data centre-specific tax and duty incentives that will encourage investors to operate here.
- ✓ Benefits like introduction of tax breaks for 10 years and special power tariffs should be offered, considering these institutions run the Digital India and e-commerce backbone of India and need huge amount of capital investment

RELIANCE JIO INFOCOMM LIMITED ★

- ✓ Land should be provided at special rates with faster clearances given to data centre building proposals
- ✓ Special subsidized provisions of high capacity power availability should be given to data centres
- ✓ Zero duty import of IT equipment for data center hosting and cloud companies should be ensured
- ✓ The government should promote investments on IT infrastructure which will motivate entrepreneurs to adopt new technologies
- ✓ Introduction of special monetary incentives be made for companies to invest in research and development
- ✓ Subsidise Power Rates-Singapore and the US are preferred over India by startups owing to high costs associated with power in India. Subsidy in power is a must to bring down prices which will encourage and enable MNCs to set up or collocate with companies for doing business in India
- ✓ India can also create a special zone for promoting DC builds with additional tax SOPs. The zones could include the suitable remote locations where businesses could be encouraged to set up DCs. This will not only solve the purpose of making the DCs safety provisioned but will also lead to economic development in that region.

****

RELIANCE JIO INFOCOMM LIMITED ★