Reliance Communications Limited's Response to the

Consultation Paper on Cloud Computing

Executive Summary

A. **The paradigms of cost benefit, for the cloud based services apart from financials, is in terms of time to market the product, scaling of services as per demand, economical services since you pay as you go and Always On and available Anywhere and Anytime on the device of the users choice.**

B. **Adoption of cloud computing setup is better economic prudence vis-a-vis an in house IT setup. The benefits are accrued on two counts, (a) Directly - through reduced costs on account of IT Infrastructure and Power and (b) Indirectly - by increased focus on core business functions.**

C. **Key factors to be considered while selecting the type of cloud service deployment model are (a) In house Skills of the organization, (b) Business use case requirement, (c) Roll out time lines and Go to market strategy, (d) Compliance and Control requirements and (e) Cost, ROI period and business value.**

D. **In case the application and its database is being migrated outside the territorial boundaries of India, both the CSP and the application owner should be mandated to inform the DoT before initiating the migration process.**

E. **Irrespective of the type of migration, before initiation of the migration of services, establishment and migration of services to the Disaster Recovery (DR) set up should be mandated, especially for the applications that require live migration.**

F. **Signing of appropriate Non Disclosure Agreements and compliance of DoT's guidelines for Remote Access should be mandated, especially if the third party vendor is being requisitioned from outside the territorial boundaries of India.**

G. **It is the data owner's responsibility to requisition the secured pipe and the TSP providing the secured pipe would be responsible for the security of the data while it is being transferred from one place to another.**

H. **TRAI should mandate compliance to the internationally adopted, accepted and followed codes of practices rather than developing a new regulatory framework to cover cloud computing issues such as data ownership, information security, etc.**

I. **The interoperability clause should be under a mutually agreed, contractual agreement between the CSPs and the customers and should not be under any regulatory framework.**

J. **The government can consider establishment of an Interoperability test bed that can help assess the commitment to "openness" of each CSP.**

K. **The QoS requirements for the cloud services should be kept under mutually agreed contractual agreements between CSPs and the customers.**

L. **Cloud Service providers should maintain a detailed log capturing the customer's ID, action(s) taken (new subscription, deletion, modification, administration action etc), timestamp(s) of actions and logical address of the source device, for at least 6 months, so that complete audit trail and record is available for any dispute resolution.**

M. **CSPs should be subjected to mandatory billing and metering audit through government / regulatory body accredited auditors similar to the practice being followed for the Telecom operations.**

N. **It should be mandated for the CSPs to establish a customer support team and advocate its accessibility through requisite means for both B2B abd B2C customers.**

O. **Requisitioning of level of customer support service, above a set of basic services, should be left to mutual agreement between the B2B customer and the CSP.**

P. **From a regulatory perspective, a self certification regime, that has international as well as any India specific certifications, needs to be established for self accrediting of the CSPs for instilling confidence amongst the cloud services subscribers.**

Q. **A detailed exit clause elucidating the exact exit / migration process, especially for continuity of customer's services and specification of measurable metrics, should be mandated to be part of any agreement between the CSP and the customers.**

R. **It is imperative that the laws for ensuring the security of the data, privacy of an individual and necessary disclosures to introduce transparency are also enacted as, Global level / Bilateral agreements which are bounden on all the stakeholders of the cloud computing services eco-system.**

S. **India should have maximum possible number of "Mutual Legal Assistance" agreements.**

T. **India should encourage local hosting of servers and applications.**

U. **Cloud computing should not be subjected to the Indian Telegraph Act 1885 and should be dealt with a light touch regulatory regime with no requirement of licensing / registration.**

V. **Exclusive cloud setup hosting only the governmental services should be mandated in any type of cloud deployment model.**

W. **The cloud setup established for provisioning government services can be hosted in the government data centers or can be hired from private operators.**

Preamble

1. Computing clouds have undeniably been one of the most disruptive technology for almost each and every kind of business. Their services oriented business model has led to transformation of the traditional business models and structures. Even for the individual customer, the advent of computing clouds ushered in the era of 'always on', 'always connected devices' and emergence of 'always logged on' users.

2. Consequently, these computing clouds have become the main stay for provisioning modern Information Technology Enabled Services (ITES). Computing clouds and services being provisioned through them have typically eased the business environment resulting in creation of ITES behemoths. Apart from their brand, these businesses have data as their only tangible asset which is being continuously generated either by the activities of the users of these computing cloud based services (Tracking of movements, tracking of net surfing, M2M enabled cars, etc) or by the users themselves (selfies, messages, e-mails, videos, etc). However, **the paradox here is that though this generated data is personal to the user, but its ownership is claimed by the computing cloud based application service**

providers. At times a bigger paradox in this scenario is that even the physical cloud infrastructure too is not owned by these computing cloud based application service provider.

3. Echoing the same, the 2016, 'World Development Report – Digital Dividends' by World bank, in its section on "Analog complements for the digital economy" (subsection titled "Tailor 'new economy' regulations to ensure competition"), states that *"Internet firms create new business models and change market structure, posing new challenges for regulatory authorities. On-demand economy firms like Uber and Airbnb scaled up traditional ride sharing and subletting to a global scale. But regulators struggle to determine whether these companies are taxi or hotel companies or simply software providers. Similar regulatory puzzles are posed by firms such as Amazon, Facebook, and Google. For example, Google is known as a search engine company but is better described as an advertising firm. These firms confound conventional competition law because they do not act as traditional monopolies. Their services are often free to consumers. Research by economists such as Jean Tirole has shown that regulations in such industries must be carefully tailored to guarantee competition and avoid harm to consumers. These are very challenging problems, and most pressing in the transforming countries"*.

4. From India's perspective, the country is an exponentially growing market for ITES. The availability of youthful population and a sizable IT skilled manpower, India has proved to have immense appetite for these ITES. **The fact that India has achieved the distinction of being the second or the third largest subscriber base for most of the popular ITES, has also made it a net exporter of data bytes / information.** With the introduction of M2M services, the data / information exporting scenario is only going to get accentuated further. With the second largest startup ecosystem and fast emerging e-commerce platforms, the importance of data and its hosting infrastructure is going to increase many folds. Some experts have in fact predicted that **data is going to be the currency of the future.**

5. **An inherent implication of being a net data exporter is that India as well as its citizens can be vulnerable to external forces inimical to the country's interests.** There is already a lot of talk about weaponization of the internet wherein, data can be the future tangible tradeoff material between the opposing parties.

6. As per the 2016, 'World Development Report – Digital Dividends' by World bank, "*Some countries are considering regulations that make it legally binding for data of or about their citizens to reside within their national borders, also referred to as data localization or data nationalism. While such barriers may stem from legitimate concerns about privacy and security for their citizens' information, they can be costly".*

7. The above mentioned intricacies of computing cloud based services providers coupled with the fact that the physical infrastructure utilized for provisioning their services are globally location agnostic create a challenging situation for the local licensing and regulatory authorities for regulating the entire computing cloud eco-system including their services. Given India's current status of the fastest growing economy, **it is imperative that the guidelines for regulation of computing clouds not only build adequate safeguards for ensuring the security and safety of the data as well as an individual's privacy but also ensure that the largest data consumption areas transform into net data importers for the other parts of the globe. It is also equally imperative to ensure that the regulator's policies should not stifle innovation and creativity while indulging in over protectionism of the users / well established cloud computing based services providers.**

8. Our specific comments on the issues posed by the Authority are given in the subsequent paragraphs.

Detailed Response

Question 1: 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.

Our Response

1. Cloud Computing is a paradigm where computing resources are characterised by,
    a. Always On, Anywhere and Anytime.
    b. Available when needed.
    c. Pay As you go. (One can use and pay for the use of computing resources for as much or as little as one uses.)
    d. “No-need-to-know” the underlying complexity and details of the computing infrastructure.
    e. Similar to the house hold utilities like water and electricity, when we turn off the usage of the cloud computing resources, the same are made available for use by others.
2. Apart from the requirement of just a skeletal IT team that is required for coordination with the CSP, organizations no longer need an elaborate internal IT department i.e. people who aren't core to the products and services. Organizations can stop worrying about hiring and retaining a premium workforce with IT skills and are spared from the requirements of tracking and implementing upgrades / avoiding obsolescence of the hardware, OS and applications. e.g. Travel companies / airlines have peak periods before and during holiday season. To provide services during these days traditionally they used to invest upfront in IT infrastructure in advance with some predicted load. This may be oversized or undersized based on the actual business during the season. Cloud services now allow them to realign resources basis the demand on the fly ensuring IT infrastructure in line with the business demand. Ecommerce benefits the same way from Cloud Services. To summarize based on business demand resources are provisioned and costs are incurred making efficient use of money resources

3. As per the opengroup.org website[1], "the key practical differences between traditional computing environments and cloud computing are shown below".

Characteristic	Cloud Computing	Traditional IT Setup	Comments
Time before service can be accessed	Minutes / Hours	Days / Weeks	Once the cloud computing environment is set up initially, you can gain access faster than in traditional environments where lead time is needed for installation, set-up, and configuration.
Capital Expenditure (CAPEX)	Pay-as-you-go, Variable	Upfront cost, Fixed	The pay-as-you-go model for cloud computing reduces or eliminates the large upfront costs incurred in procuring hardware and software and standing up traditional environments.
Economies of scale	Yes, for all organizations	For large organizations only	Cloud computing not only provides cost advantages in procurement of hardware and software, it also provides cost advantages from improved productivity. Traditionally, lessons learned from one environment must be duplicated in other environments but, with cloud computing, once the best practices are applied they benefit all consumers.
Multi-tenancy	Yes	Generally no, but can be found in application hosting	Multi-tenancy properly applied to cloud computing services allows providers to host multiple consumers effectively across shared resources. While it is more readily enabled in IaaS through the use of virtualization, PaaS and SaaS providers may need to undertake significant re-architecting of their platforms or applications to apply multi-tenancy to these elements as well as to infrastructure. Where this has not been undertaken, consumers may find that their platforms and applications are not as elastic or cost-effective as anticipated.
Scalability	Elastic and Automatic	Manual	Cloud computing resources can often be scaled up or down automatically, whereas human intervention is usually needed to add hardware and software in traditional environments.
Virtualized	Usually	Sometimes	Cloud computing environments are usually virtualized, whereas traditional environments include a mix of physical and virtualized infrastructure.

Table 1: Showing Practical Differences between Cloud Computing and Traditional Environments
Source : http://www.opengroup.org/cloud/cloud/cloud_for_business/what.htm

[1] http://www.opengroup.org/cloud/cloud/cloud_for_business/what.htm

4. In an enterprise that has complex and expensive IT systems to support its business processes, **the paradigms of cost benefit, for the cloud based services apart from financials, is in terms of time to market the product, scaling of services as per demand, economical services since you pay as you go and Always On and available Anywhere and Anytime on the device of the users choice, as shown against each in the table below.**

Ser No	Requirement	Time to Market Support	
		Cloud Computing	**Traditional IT Setup**
1	Accelerating the Design & Roll out of services	1. PaaS can be requisitioned for instantaneous implementation of the idea within Hours / Days / Weeks. 2. IaaS, PaaS, SaaS can be requisitioned for immediate launch of services. 3. SDK environments and contributions from the Open source communities facilitate faster development of applications. 4. ROI comparison across IaaS, PaaS & SaaS and between private / public / hybrid deployment models facilitates optimal and faster decision for adoption.	Implementation schedule cloud stretch from within Weeks / Months depending on the existing availability of IT setup, to Years if the set up has to be established from scratch.
2	Promotion of Social Networking	1. Services are Always On and available Anywhere and Anytime on the device of the users choice. 2. Elastic Resource availability ensures that the scaling up and down of the IT support setup can be effected instantaneously as per the increase / decrease in subscribers accessing the services. 3. Pay as you go enables economical services provisioning. 4. The availability of cloud based services being device agnostic, it enables increased outreach and transparency resulting in increase in participatory governance. E.g. Governments latest initiative for provisioning open data will have to be implemented as a cloud based services. 5. Ubiquitous availability of localized content, across devices, will help promotion of Social Networking, Participative Governance and E-commerce.	1. Difficult to model the demand and consequently the IT setup resulting in under / over provisioning of computing resources. 2. Under / Over provisioning of resources shall lead to wasteful expenditures on account of enhancing the setup or the resources being idle resulting in economically sub optimal services.
3	Participative Governance		
4	E-commerce		
5	Expansion of new services	1. Elastic Resource availability ensures that the scaling up and down of the IT support setup can be effected instantaneously as per the increase / decrease in subscribers accessing the services. 2. Pay as you go enables economical services provisioning. 3. Help end-user organizations, including SMEs, to enhance reliability of services through implementation of services like Disaster Recovery and High Availability at low cost.	

Table 2: Showing paradigms of cost benefit between Cloud Computing and Traditional IT Setups

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

Our Response

1. In a Pennsylvania State University Paper "To Move or Not to Move: The Economics of Cloud Computing" by Byung Chul Tak, Bhuvan Urgaonkar and Anand Sivasubramaniam, they have classified cost of an IT setup of an organization into direct and indirect costs. As per the paper, some portion of each of these costs is clearly quantifiable whereas some is less quantifiable as shown in the Figure 1.

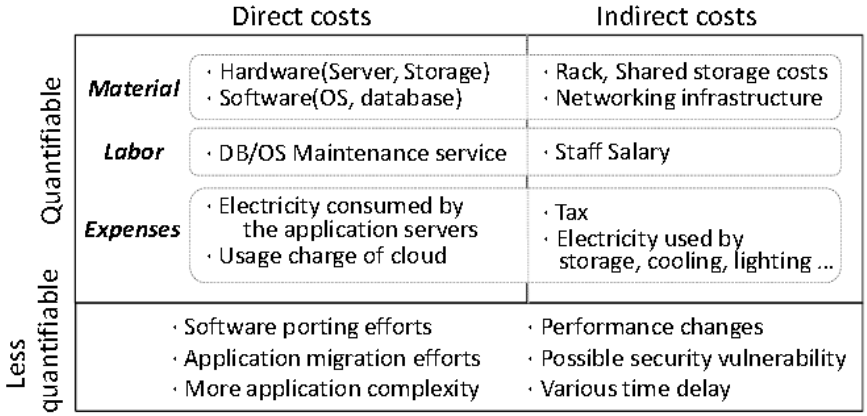

Figure 1: Showing Classification of Cost for an IT setup

Source: Pennsylvania State University Paper "To Move or Not to Move: The Economics of Cloud Computing" by Byung Chul Tak, Bhuvan Urgaonkar and Anand Sivasubramaniam

2. As per a study titled "Cloudonomics: The Economics of Cloud Computing' from Diversity and rackspace hosting, the 80-20 rule aptly explains the utilization of IT resources in the organization. This study *"hypothesize that only 20% of the time and effort that goes into running applications, where all business value is concentrated, is actually concerned with running those applications themselves. The diagram below illustrates the extent that routine and non-core tasks, like patching operating systems and performing backups, impact upon the time of IT departments"*.

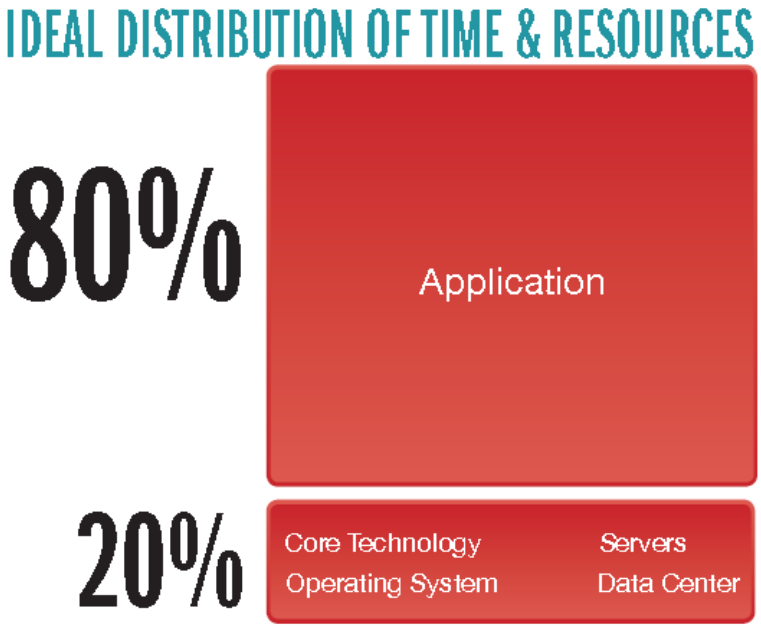

Figure 2 : Showing the Ideal Distribution of Time & resources for an inhouse IT environment

Source: Cloudonomics: The Economics of Cloud Computing' from Diversity and rackspace hosting

3. Cloud Service Providers build large scale IT infrastructure for consumers and enterprise customers. The sheer volume of the IT infrastructure makes an impact on the cost at which they source the same. CSPs further optimize the pricing by building an optimized pool of compute resources orchestrated with an automation layer. This approach ensures maximum utilization of available resources enabling faster RoI which is not possible to achieve at smaller scales. CSPs pass on these benefits to customers in terms of pricing and by enabling on-demand resource provisioning and auto-scaling options to keep operational costs for customers in line with business demand resulting in cascading of the RoI for the customers as well.

4. Consequently, the 'Resource Pooling' characteristic of cloud computing has resulted in significant IT cost savings through effecting a shift in the business and economic models for provisioning and consuming information technology (IT). Cloud computing economics depends on four customer population metrics as given below.
   a. Number of Unique Customer Sets (n).
   b. Customer Set Duty Cycles (λ,f).
   c. Relative Duty Cycle Displacement (t).
   d. Customer Set Load (L).
5. Maximum level of IT resource demand is possible to be serviced through the use of minimum amount of physical IT resources by optimal exploitation and balancing of these metrics. It is estimated that a data center functioning with the correct balance amongst these factors has the ability to realize an approximately 30% savings in IT resources.
6. A 2009 Booz Allen Hamilton (BAH)[2] study concluded that a cloud computing approach could save 50 to 67 percent of the lifecycle cost for a 1,000 server deployment. For the study, Booz Allen team created a detailed cost model that had capabilities for creating the Life Cycle Cost (LCC) estimates for public, private and hybrid clouds. They used the following three key metrics for their analysis.
   a. **Net Present Value (NPV)** i.e. the cloud model's reduced O & S costs relative to the Status Quo (SQ) environment's O & S costs.
   b. **Benefit-to-cost ratio (BCR)** which was calculated as each cloud model's discounted net benefits divided by its discounted investment costs.
   c. **Discounted Payback Period (DPP)** which reflected the number of years it would take for each model's accumulated annual benefits to equal its total investment costs.
7. The economic results (summarised at the bottom portion of the Table 1) clearly show that the projected NPV and BCR for all these models are significant relative to the SQ environment. Their model suggested that once the migration to the cloud computing environment would be completed there would be annual O & S savings of approximately 65% – 85%. Using this BAH study as a guide, Forbes magazine, for an article in cloud economics, had calculated that the transitioning of IT services from an agency owned IT infrastructure to the CSP IaaS platform could deliver benefit cost ratios of approximately 7:1.

[2] The Economics of Cloud Computing : Addressing the Benefits of Infrastructure in the Cloud by Ted Alford and Gwen Morton.

Costs/Economic Metrics	Status Quo: 1,000 Server (Non-Virtualized) Environment	Scenario 1: Public Cloud	Scenario 2: Hybrid Cloud	Scenario 3: Private Cloud
Investment Phase Costs FY10–12 (BY09 M$)	$0	$3.0	$6.1	$7.0
O&S Phase Costs FY10–22 (BY09 M$)	$77.3	$22.5	$28.9	$31.1
Total LCCs (BY09 M$)	$77.3	$25.5	$35.0	$38.1
Economic Metrics:				
NPV (BY09 M$)	N/A	$41.8	$33.7	$31.1
BCR	N/A	15.4	6.8	5.7
DPP (Years)	N/A	2.7	3.5	3.7

Table 3 : Showing LCCs and Economic Summary of the results obtained through the model created in the BAH Study
Source: Booz Allen Hamilton Study on economics of cloud Computing[1]

8. The "Cloudonomics: The Economics of Cloud Computing' from Diversity and rackspace hosting study contends that, "*There are many reasons for organizations to move from traditional IT infrastructure to Cloud Computing. One of the most cited benefits is the economics of the Cloud. Yet while many people point out the cost savings that Cloud Computing brings to an organization, we believe attention should be drawn to four distinct mechanisms through which these cost savings are generated:*

   a. ***By lowering the opportunity cost of running technology".*** The study applies the concept of 'Opportunity Cost' (The basic economic premise is concerned with the costs related to the choices NOT made by someone), to cloud computing and assesses the economic benefit of the true cost of any potential action of adopting cloud based services vis-a-vis deploying own infrastructure. It concludes that *"a move to the Cloud can make the difference between an organization being 20% efficient, and one being 80% efficient".*

   b. ***"By allowing for a shift from capital expenditure to operating expenditure".*** This study has likened the yearly OPEX expenditure to the telephone or electricity expenditures. Giving a comparative table (Table 2) to highlight its point on savings from adoption of clouds, it states that, *"OpEx is beneficial for the organization, as it gives it the flexibility to terminate costs at will".*

	Internal IT	Managed Services	The Cloud
Capital Investment	$40,000	$0	$0
Setup Costs	$1,000	$5,000	$1,000
Monthly Services	$0	$4,000	$2,400
Monthly Labor	$3,200	$0	$1,000
Cost over three years	$149,000	$129,000	$106,000
Savings Gained	0%	13%	29%

Table 4 : Showing Estimated costs of infrastructure for 2 x application & DB servers each, a LB across different Cloud deployment models.
Source : (a) http://broadcast.oreilly.com/2008/10/the-economics-of-cloud-c.html for more information about the economics of Cloud Computing and (b) http://gigaom.com/2010/06/06/lazy-hazy-crazy-the-10-laws-of-behavioral-cloudonomics/

c. ***"By lowering the total cost of ownership (TCO) of technology".*** In an article published by Bernard Golden[3] at CIO.com, Bernard has pointed out that *"calculations of in-house costs fail to take into account,*

i. *The direct costs that accompany running a server: power, floor space, storage, and IT operations to manage those resources.*

ii. *The indirect costs of running a server: network and storage infrastructure and IT operations to manage the general infrastructure.*

iii. *The overhead costs of owning a server: procurement and accounting personnel, not to mention a critical resource in short supply: IT management and its attention."*

d. As per this study, the adoption of cloud computing has the advantage that *"most costs are upfront and readily calculated; this is due to a number of factors,*

i. *Cloud providers give transparent pricing based on different usage metrics – RAM, storage, bandwidth, among others.*

ii. *Pricing is frequently fixed per unit of time. Customers gain certainty over pricing and are then able to readily calculate costs based on several different usage estimates."*

e. ***"By giving organizations the ability to add business value by renewed focus on core activities".***

9. **Power.** There are power and cooling losses in each hop from distribution source to IT infrastructure. Various studies have revealed that on an average, for a data center with a PUE of 1.5, the cooling losses are almost to the tune of 22%. However, **a well designed, energy efficient data center can optimize the power costs and enable distribution of the cooling burden on a larger number of customers.** Consumers can simply leverage these strengths of the data centers and enhance their focus on their core business.

Our Conclusions

10. As can be inferred from the foregoing discussion, **adoption of cloud computing setup is better economic prudence vis-a-vis an in house IT setup. The benefits are accrued on two counts, namely,**

a. **Directly - through reduced costs on account of IT Infrastructure and Power.**

b. **Indirectly - by increased focus on core business functions.**

11. **The amount of cost savings is directly proportional to the scale of the data center and the time taken to shift operations into the cloud.**

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?

Our Response

1. Choosing the type of cloud service deployment model that best suites an organizations business objectives is a multi-dimensional problem. Apart from the enormous economic payoffs, Cloud Computing offers significant extra value to organizations by allowing them to focus on their core business. In fact this value side of the equation is, most often, even more

[3] http://www.cio.com/article/484429/Capex_vs._Opex_Most_People_Miss_the_Point_About_Cloud_Economics

compelling than any cost savings possible. Each type of Cloud computing model provides its own strong benefits and economic incentives. E.g. Organizations having in house IT skills to build and manage IT Applications, may opt for IaaS. Software development companies developing applications may want to have development setup on PaaS so that they don't spend time managing underlying infrastructure and platform. Customers who intend to only use certain applications and don't wish to look at underlying infrastructure and platforms will choose SaaS. It should be noted that it is not only the organization profile and in house skill availability, but also about the use case and business value looked for. Organization may have in house skills to build and manage applications but based on business service rollout and go to market strategy they may choose to go for a ready to use SaaS solution. It may also happen that there is a ready to use application available but from compliance and control perspective, organization may want to build it in house on a IaaS layer.

2. Based on the business objectives of an organization, the selection of a public, private, hybrid or community cloud implementation will depend on the following specific criteria as listed below.

   a. **Ubiquitous Broad Band Connectivity.** Broadband service provider agnostic cloud computing facility providing connectivity with guaranteed performance at a reasonable cost, is ideal as it affords ubiquitous access to all internet subscribers.

   b. **Security**

      i. **Physical Infrastructure and Compliances.** A well secured cloud computing hosting facility complying to international security standards such as ISO 27001, etc is most reassuring for the prospective client.

      ii. **Data.** It is imperative not only from the CSPs client perspective but also from the perspective of the subscribers of the hosted services and legal requirements.

   c. **Performance.** Achieving high-speed delivery of applications in the cloud is a multifaceted challenge that requires a holistic approach and an end-to-end view of the application request-response path. Performance issues include the geographical proximity of the application and data to the end user, network performance both within the cloud and in-and-out of the cloud and I/O access speed between the compute layer and the multiple tiers of data stores.

   d. **Multi Tenant Environment.** The host server of the cloud computing services provider has virtual machine (VM) of multiple clients running concurrently. Therefore, the public / hybrid cloud providers do not provide access to the hypervisor resulting in the clients inability to be able to install host-level utilities, such as antivirus software or backup agents. This also means that the client is not able to join a hypervisor to an existing domain or cluster. Apart from this there are also security implications, as well as the possibility of potential downtime from cloud or WAN failure.

   e. **Resiliency and Redundancy.** A resilient and redundant infrastructure ensures robustness and translates into availability of services for the maximum time.

   f. **Technology Stack.** Basically pertains to the realm of Platform as a Service (PaaS). If an application is built using one of the stacks such as Heroku and Engine Yard for Ruby on Rails; VMforce and Google App Engine (GAE) for Java/Spring (GAE also supports Python), PHP Fog for PHP and Microsoft's Windows Azure for .NET, considering the cloud platform can offer tremendous savings in terms of time and expense. The flip side is that

they often require developers to follow certain best practices in architecting and writing their apps, which creates a higher degree of vendor lock-in.

g. **API: Lock-in, Community and eco-system.** Exposition of Application Programming Interface (API) for accessing the infrastructure and performing operations such as provisioning and de-provisioning servers is a critical aspect of adopting a cloud computing model. The API is important in a number of ways as,

   i. An API that is supported by multiple providers and vendors reduces lock-in and supports migration from one cloud computing infrastructure to another / simultaneously multiple cloud based working environment and hence requires less change to the application and is, therefore, easier.

   ii. An API that is widely supported by a community of developers and vendors has an entire ecosystem around it of complementary services and capabilities.

h. **Storage and Backup.** The response time of the cloud computing infrastructure's Storage Area Network (SAN) and its ability to backup data and provide restoration facilities is an important consideration while short listing the model of cloud computing for adoption.

i. **SLA and Reliability.** Though, SLAs are often merely an indication of the consequences when the service fails and not the service's actual reliability, however, the level of SLA's offered by a cloud computing service provider is a good indicator of its level of commitment for reliable services.

j. **Civil Infrastructure and Allied Facilities.** The quality of civil infrastructure and allied facilities is important to ensure reliability of the cloud computing infrastructure.

k. **Ease, Flexibility and Elasticity of Service Access and Requisition.** One of the most important consideration as it enable prompt response to any surge / decline in requirement of resources as and when the need arises.

l. **Ease of Billing and Billing Verification.**

m. **Data Analytics Capability.**

n. **Ease of monitoring (Availability of reports with analysis including RCAs)**. The cloud computing services subscriber organization is reassured of the quality of services that the CSPs is providing if it is able to monitor the health of the infrastructure on which their application is hosted.

o. **Cost.** By far the most important factor for any consideration of adopting the type of cloud computing model. The economics of hosting in a cloud infrastructure has already been discussed in detail in our response to question no 2.

Our Conclusions

3. Balancing the above mentioned criteria, an organization is able to determining the right cloud computing model that it should adopt for most ideally meeting its business objectives. However, **one of the main criteria for selection of the cloud computing model is the capital available with the organization.** In any organization, acquiring capital for large purchases is difficult, especially for smaller organizations for which finance companies apply rigorous debt to equity ratios limiting the amount of capital that they can acquire. While larger organizations with adequate CapEx support would able to establish their own private

enterprise clouds, moving to an OpEx model removes this limitation and allows small scale projects to be undertaken, unconstrained by capital considerations.

4. To summarize **following are key factors to be considered,**
    a. **In house Skills.**
    b. **Business use case requirement.**
    c. **Roll out time lines and Go to market strategy.**
    d. **Compliance and Control requirements.**
    e. **Cost, ROI period and business value.**

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?

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

Our Response

1. There are multiple factors to be considered when it comes to deployment / migration from one cloud to another cloud. Cloud is an evolving model and different technologies have evolved along the way. While there has been an effort on defining standard methods and formats it will take very long time to establish uniform methods and interoperable deployments. As on date migration should be viewed from the Cloud Service deployment model perspective, sic,
    a. IaaS.
        i. VM image should support open format to port it on other cloud platforms.
        ii. Data volumes should be backed up with tools used by customer so that they can restore the same and have continuity on backup catalogue.
    b. PaaS & SaaS.
        i. These are complex environments and each service provider has there own platforms, middleware and application layers and portability will be a challenge.
        ii. Each service provider has a different method for integrating different service components thru APIs.
        iii. Customers should check on input and output data formats and based on the same check with other service providers to provide same capability.
2. Migration to a cloud setup or migration from one cloud setup to another is a decision that can have major ramifications for the entire business of an organization or even for national interests. Therefore, any decision to migrate to or from one cloud setup to another has to clearly define the following,
    a. **KPIs or SLAs for migration.**
        i. The definition of the KPIs or SLAs has to be based on the delay tolerance level of an application being migrated instead of the business scenario or the customer environment.

ii. **Customers should have clause in the agreement to provide customer's data in open formats so that it can be imported by other cloud providers supporting same open format.**

iii. **In case the application and its database is being migrated outside the territorial boundaries of India, both the CSP and the application owner should be mandated to inform the DoT before initiating the migration process.**

b. **Appropriate type of Migration.** Based on the criticality of the application, the migration process needs to be decided as (a) Offline Vs Live in Real Time and (b) with user involvement Vs opaque to the user. E.g For applications that are live and cannot be shut down, like the payment portals, etc, it is imperative that the application is made available to the environment without any break in service and hence, have to be mandatorily migrated live. Whereas on the other hand, applications such as e-commerce shopping sites may not have very stringent live migration requirements, from criticality point of view, and can be migrated offline as well. **Irrespective of the type of migration, before initiation of the migration of services, establishment and migration of services to the Disaster Recovery (DR) set up should be mandated, especially for the applications that require live migration.**

c. **Roles and Capabilities of the stakeholders involved in the migration process.** Apart from the roles of the CSP and the customer, it is important to define the roles of the third party vendors whose services might be requisitioned for preparing the data and the application for migration. **Signing of appropriate Non Disclosure Agreements and compliance of DoT's guidelines for Remote Access should be mandated, especially if the third party vendor is being requisitioned from outside the territorial boundaries of India.**

3. It is brought out that the migration of cloud services entails manual intervention as well as utilization of automated tools and scripts. Security of the specific manual actions as well as the tools and scripts being used and their output should be defined in unambiguous terms and implements by the organization that is responsible for that aspect of the migration process. E.g.

a. **Security of Compute Elements** like VMs, VM images, Pre-built application images, License security, etc should be that of the CSP.

b. **Data and Storage Security.**

i. <u>At rest.</u> The CSP should be responsible for the security of the data and the storage while it is stored in the discs.

ii. <u>During movement / migration.</u> It is imperative that the data be transferred through secured pipes. Accordingly, it is the **data owner's responsibility to requisition the secured pipe** and the **TSP providing the secured pipe would be responsible for the security of the data while it is being transferred from one place to another.**

iii. Along with context / state or without.

c. **Network Path Security.** The Network path provider i.e. the TSP shall be mainly responsible for securing the path between the source and destination cloud setups. Securing the path would entail the following.

i. Establishment of authentication and trust mechanisms between the end-points, i.e. source and destination clouds. For ensuring customer's control over the data while it is being transferred, it is imperative that the authentication and trust mechanism be shared with the customer by the TSP.

ii. Provisioning of encrypted communication channels, protocols and secure messaging. It is the customer's responsibility to requisition secured communication channels for transferring his data. However, once requisitioned, the TSP needs to ensure the implementation of proper encryption of the communication channel.

d. **Secure migration of Identity and Authentication Mechanisms.**

Our Recommendations

4. **Customers should have clause in the agreement to provide customer's data in open formats so that it can be imported by other cloud providers supporting same open format.**

5. **In case the application and its database is being migrated outside the territorial boundaries of India, both the CSP and the application owner should be mandated to inform the DoT before initiating the migration process.**

6. **Irrespective of the type of migration, before initiation of the migration of services, establishment and migration of services to the Disaster Recovery (DR) set up should be mandated, especially for the applications that require live migration.**

7. **Signing of appropriate Non Disclosure Agreements and compliance of DoT's guidelines for Remote Access should be mandated, especially if the third party vendor is being requisitioned from outside the territorial boundaries of India.**

8. **It is the data owner's responsibility to requisition the secured pipe and the TSP providing the secured pipe would be responsible for the security of the data while it is being transferred from one place to another.**

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?

Our Response

1. Migration of applications / data bases in and out of the cloud can be initiated at the behest of the customer himself or due to the CSPs requirements of storage optimization and consolidation or technology refresh cycle mandating replacement of the older storage systems. In order to ensure that the customer is able to have control over his data while moving it in and out of the cloud following measures are suggested.

2. **Legal Requirements.** Irrespective of the reason for initiation of the movement of the applications / data bases, **as a precursor approval of the data owner, before initiation of the migration process should be mandatory.** The customer, being the data owner, must have a clear statement to this effect in its agreement(s) with the CSP. Moreover, these

agreements should **clearly define the legal jurisdiction in which any disputes related to data ownership will be resolved.**

3. **Technical Requirements.** Cloud computing has been predominantly supported by a plethora of open source applications that are in an ever evolving mode. Given the dynamic nature of the cloud computing environment, maintaining information security demands a holistic approach encompassing the multiplicity of aspects that are required to be looked into for the same. Specifying a set of rigid guidelines would not be the right approach as the bindings would prevent the CSPs from maintaining technological currency for their security systems, processes and procedures. It is for these reasons that the industry best practices have opted to accredit their service offerings, by getting certified, as per standardization benchmarks set by international technology communities like ISO / IEC (International Organization for Standardization (ISO) and International Electro-technical Commission (IEC)).

4. **Example.** For migration of data it is imperative that the data is secured, privacy is maintained and the roles and responsibilities of each of the stakeholder is elucidated neutrally. Accordingly, it is suggested that the CSPs should be accredited as per the following.

   a. ISO / IEC 27018 which lists the code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. This standard requires that CSPs operate under six key principles as follows,

      i. **Consent. C**SPs must not use the personal data they receive for advertising and marketing unless expressly instructed to do so by the customer.

      ii. **Control.** Customers have explicit control of how their personal data is used.

      iii. **Transparency.** CSPs must inform customers where their personal data resides and make clear commitments as to how that data is handled.

      iv. **Accountability.** Any breach of information security should trigger a review by the CSP to determine if there was any loss, disclosure, or alteration of personal data.

      v. **Communication.** In case of a breach, CSPs should notify customers, and keep clear records of the incident and the response to it.

      vi. **Independent and yearly audit:** A successful third-party audit of a CSP's compliance documents the service's conformance with the standard, and can then be relied upon by the customer to support their own regulatory obligations. To remain compliant, a CSP is mandated to subject itself to yearly third-party reviews.

   b. ISO / IEC 29100:2011 which is applicable to natural persons and organizations involved in specifying, procuring, architecting, designing, developing, testing, maintaining, administering, and operating information and communication technology systems or services where privacy controls are required for the processing of PII. The certification provides a privacy framework which,

      i. Specifies a common privacy terminology.

      ii. Defines the actors and their roles in processing personally identifiable information (PII).

      iii. Describes privacy safeguarding considerations.

iv. Provides references to known privacy principles for information technology.

5. **Requisitioning and Provisioning trans border CSP services.** Since services of the CSPs are available seamlessly across the globe, adoption of internationally adopted, accepted and followed codes of practices shall facilitate emergence of business opportunities for Indian CSPs as well.

6. **Data Deletion Requirements.** In situations where an existing customer moves from one CSP to another or simply decides to discontinue services from a particular CSP, another important issue related to data ownership becomes critical–that of **'customer data retention' at the CSP the customer is moving out of.** The CSP must be required to state their data retention policies relevant to each level of cloud service that the customer was using. E.g. some of the key elements for which the CSPs must state their data retention policies are as follows.

   a. Customer's VM images.

   b. Customer's Application images.

   c. Customer's databases.

   d. Customer's Application level meta-data etc.

   e. The data retention / deletion clauses must cover not just online stores for such data, but also archival and any other off-line stores the CSP may be using for storing of customer data.

7. Further, it is brought out that international agencies are also looking at issues related to security of data and information. It is expected that customer data protection models will emerge for migration of cloud based data and services. Some may be regulatory and some may be based on industry self-regulation. E.g.

   a. The EU GDPR (General Data Protection Regulation) passed in May 2016 provides significant protection to the users towards – right to access, right to correction, erasure, to be forgotten and right to portability – this regulation is due for enforcement in 2018.

   b. The UK Government has observed the emergence of concept of Self-regulatory bodies. Technology companies are asking for clarity on whether self-regulatory bodies are officially recognized, to ensure the bodies are effective and reliable so that industry can consider setting them up.

Our Recommendations

8. In view of the foregoing following recommendations are suggested.

   a. **Approval of the data owner, before initiation of the migration process should be mandatory.**

   b. **Legal jurisdiction in which any disputes related to data ownership would be resolved should be clearly defined in the agreements between the CSP and the customer.**

c. **TRAI should mandate relying on a the internationally adopted, accepted and followed codes of practices rather than developing a new regulatory framework to cover cloud computing issues such as data ownership, information security, etc.**

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?

Our Response

1. The exploitation of the cost benefit of cloud computing services have enabled provisioning of vast number of innovative services. While, the CSPs are at the forefront of supporting the innovation environment, however, it is imperative to ensure that the CSPs do not introduce direct / indirect barriers for customer applications to interoperate. The modern entrepreneurs must retain their freedom and ability to innovate and create differentiation from competitors to ensure successful business operations for which interoperability of cloud services is a must.

2. Though interoperability standards are currently evolving in the cloud industry, it may be not be possible to mandate a regulatory framework and standards for the same at this stage. Therefore, it is recommended that the government can consider establishment of an Interoperability test bed that can help assess the commitment to "openness" of each CSP in the market as follows.

   a. Use of the internationally accepted Openstack as a baseline for Interoperability testing since it is emerging as a widely supported cloud API with support from many CSPs.

   b. CSPs can be asked to show how they support the following between their cloud and Openstack.

      i. Migration.

      ii. Movement of Data.

      iii. Interoperability in terms of abstraction, programming and orchestration.

   c. Each CSP can be rated based on the level of interoperability they can demonstrate, viz,

      i. Support all requirements for migration, data movement and interoperability.

      ii. Support all important requirements.

      iii. Have a roadmap to support all important requirements.

      iv. Have no plans to support important requirements.

   d. **As a business best practice it shall be in the CSPs interest to transparently declare proprietary features and functionality in their clouds that are not available in the OpenStack** to enable an informed decision by the customers as they may be locked in to a vendor with specialized features and they can decide on using that based on their business scenario.

3. **Application level interoperability.** Interoperability of cloud services can also be considered from the perspective of,

a. **Online Interoperability.** This is crucial for applications operating in a multi-cloud environment (cloud services being provisioned from multiple CSPs) wherein the application components need to interact with each other. As a best business practice, the CSPs should provide support for such applications using standard protocols and messaging / communication techniques.

b. **Offline Interoperability**. This refers more to data portability issues which have been discussed in our response to question 5 above.

4. **CSP infrastructure level interoperability.** Beyond application level interoperability, specifically for inter-cloud management, CSP API (cloud API level) should be mandated to be provided by implementing one or more of the following.

   a. **Apache Libcloud**: Python library which hides differences among cloud providers APIs and enables managing different cloud resources through a unified API.

   b. **Deltacloud API**: Abstracts differences between clouds**.**

   c. **Apache jclouds**: Open-source library to use portable abstractions or cloud-specific features.

   d. **The Dasein Cloud API**: Inspired by JDBC and it provides an abstraction for applications that wish to be written independent of the clouds they are controlling.

5. **Services Level Interoperability.** CSPs should be mandated to enable the following important capabilities to ensure interoperability between services.

   a. Open Programming environment e.g. Specifications for the language should be available openly for which reference implementations have been provided and developed in consultation with industry bodies.

   b. Orchestration should be tested in joint testbeds. Vertical integration points should be built on top of common testbed which uses common cloud underneath.

6. **International Interoperability Standards.** Internationally, cloud interoperability standards such the Open Cloud Computing Interface (OCCI) are being adopted as they are based on the fundamentals of Representational State Transfer (REST) approach[4] of the World Wide Web, for interacting with services. OCCI is also compatible with existing standards such as the Open Virtualization Format (OVF) and the Cloud Data Management Interface (CDMI)[5]. It not only covers Infrastructure-as-a-Service (IaaS) based offerings but the interface can be extended to support Platform and Software as a Service offerings as well[6]. Therefore, it is suggested that **the regulatory framework and standards for ensuring interoperability of cloud services should be prescribe adherence to such interoperability standards instead of having proprietary, India specific standards.**

[4] http://www.ics.uci.edu/~fielding/pubs/dissertation/rest_arch_style.htm
[5] https://www.infoq.com/articles/open-interoperable-cloud
[6] A. Edmonds, T. Metsch, and A. Papaspyrou, "Open Cloud Computing Interface in Data Management-related Setups," Springer Grid and Cloud Database Management, pp. 1–27.

Our Recommendations

7. This being a highly complex area, it needs further maturing of the cloud services to regulate the interoperability amongst clouds. Therefore, in view of the above, following are recommended,

    a. **The interoperability clause should be under a mutually agreed, contractual agreement between the CSPs and the customers and should not be under any regulatory framework.**

    b. **The government can consider establishment of an Interoperability test bed that can help assess the commitment to "openness" of each CSP.**

    c. **As a business best practice it shall be in the CSPs interest to transparently declare proprietary features and functionality in their clouds that are not available in the OpenStack.**

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.

Our Response

1. The QoS parameters based on which the performance of different cloud service providers could be measured for different service models can be of two types, viz,

    a. **Dynamic Parameters.** They typically include things related to performance and speed of operations, latency, elasticity of the setup, etc.

    b. **Static Parameters.** They can include things like quality of DR capabilities, Geographic spread, Compliance with industry specific standards, Ease of use, Security capabilities etc.

2. Additionally, our response to Question 3 above, also lists several parameters that help evaluate a cloud service deployment model or a specific service. Those parameters along with the ones listed here can be used to comprehensively measure the performance of each cloud service provider.

Our Recommendation

3. Though appropriate scores can then be assigned to each CSP to measure them against the set of pre-defined QoS parameters, however, it is felt that defining QoS benchmarks for each and every aspect of a cloud services and as per the typical requirements of most of the customers, based on their budget availability and business use case, would be counterproductive. Therefore, it is recommended that **the QoS requirements for the cloud services should be kept under mutually agreed contractual agreements between CSPs and the customers.**

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?

Our Response and Recommendations

1. Billing and metering for any service is related to building the trust between the service provider and his customers. For cloud services, since the metering and billing is dependent on the consumption of data bytes, it is highly possible to establish a system of corroboration and correlation using the inputs from multiple network elements' management systems.

2. However, the importance of facilitating billing and metering re-verification by the client of Cloud services cannot be underplayed and it should be mandated to be provisioned to the customers. Following are recommended for the same.

    a. **Cloud Service providers should maintain a detailed log of online actions executed for the customer.**

    b. **These logs should capture customer ID, action taken (new subscription, deletion, modification, administration action etc), timestamp and source device logical address so that complete audit trail and record is available.**

    c. **These logs should be stored for 6 months for record keeping and dispute resolution.**

    d. **Customer should have easy access to this data and in case of any dispute both parties can review these logs together and come to a mutual consensus to resolve the dispute.**

    e. **Customers should be provisioned Instantaneous / periodic feedback to the about their usage.**

    f. **Provisioning of a trusted, may be government approved, third party tools / mechanisms for measuring the consumption of data at the user's end, similar to the apps that are available for measuring data consumption in a user's handset.**

    g. **CSPs being subjected to mandatory billing and metering audit through government / regulatory body accredited auditors similar to the practice being followed for the Telecom operations.**

    h. **Establishment of a billing dispute resolution ombudsman mechanism.**

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

Our Response

1. Cloud services providers being unlicensed have no obligation for provisioning customer care. Though CSPs have a customer support function for the B2B customers wherein the B2B customers can log their complaints and resolution process, however, the B2C customers are mostly devoid of this facility. E.g. if a Whatsapp call is of poor quality or the messaging service does not perform as per its stated functions, the customer is left to fend for himself.

2. Lack of customer support is one of the reasons for the slow uptake of the cloud services. Therefore, each CSP must be mandated to provision a separate customer care department that defines the customer's point if contact with the cloud service provider for the B2C customer as well as an escalation paths in case of continuing issues for the B2B customers.

Our Recommendations

3. **It should be mandated for the CSPs to establish a customer support team and advocate its accessibility through requisite means for both B2B abd B2C customers.**

4. **A CSP provisioning paid services for the B2C segment should be mandated to provision customer support similar to what the TSPs are mandated to provision.**

5. **Requisitioning of level of customer support service, above a set of basic services, should be left to mutual agreement between the B2B customer and the CSP**.

6. **An external agency or a central mechanism like an Ombudsman for resolution of issues of cloud services should also be established.**

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.

Our Response

1. As brought out in the preamble above, the most important tangible asset that needs to be secured in a cloud computing and services environment is 'Data'. In this cloud computing eco-system, it is user who is the generator of data, the application provider is the data processor or controller and the CSP with storage capacities is the data repository or the custodian. The main requirement in ensuring secure cloud services is that the ambiguity that is induced due to the paradox of data ownership, as elucidated in the preamble, needs to be removed and the responsibility for securing the data between the generator, controller and custodian is required to defined clearly.
2. Given the plethora of cloud services provisioning models, viz IaaS, PaaS, SaaS and their variants which can be offered through multiple combinations of deployment models viz Private, Public and Hybrid, elucidating an exhaustive list of provisions that need to be put in place to ensure that cloud services being offered are secure is a daunting task. The CSA's guide has illustrated the mapping of the cloud deployment models to the security controls and compliances as shown in the figure 5 below.

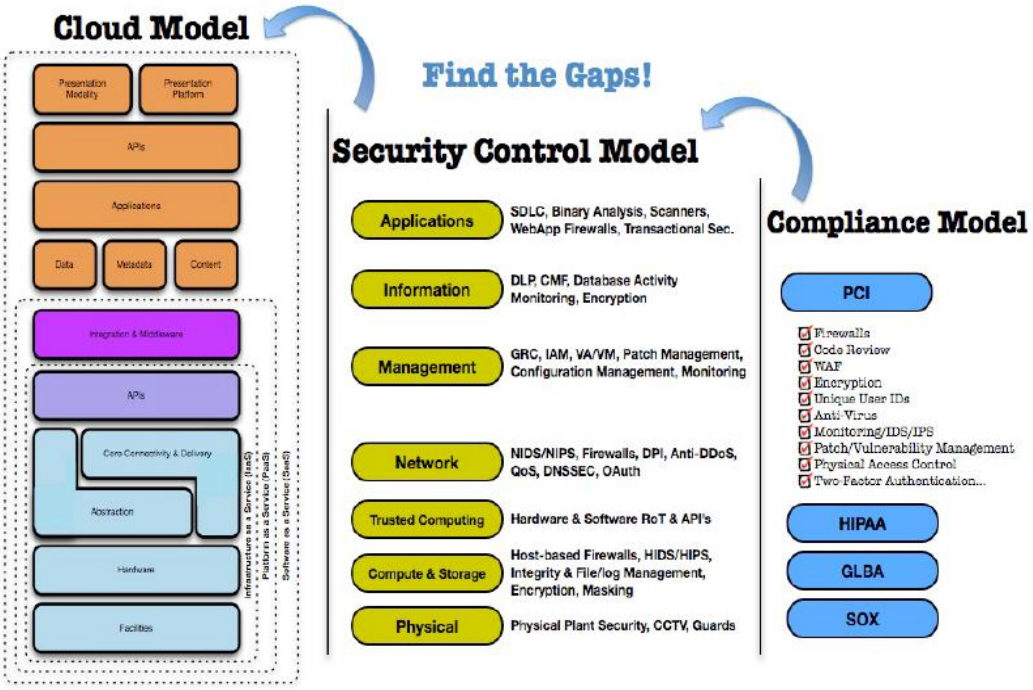

Figure 3 : Showing the mapping of the cloud models to the security controls and compliances
Source: CSA Security Guidance for critical Areas of focus in Cloud Computing V3.0[7]

3. The most important impediments for adoption of cloud computing by any organization are the lack of confidence about the security of data, performance of their application, especially in a shared environment and the reaction ability and capabilities of the cloud services provider's team in times of crisis. In order to instil confidence in the users of cloud services, it is important to ensure that the user has assurances on account of the security governance, risk management and compliance from the CSP.

4. A suggested list of provisions that should be put in place for ensuring that the cloud services being offered, by the cloud service provider are secure, is as given below. By no means is this list exhaustive and there is a need to add more provisions to it.

   a. Mandatory hosting of services within for a user base greater than 1 million.

   b. Mandatory VAPT for all equipment, be it of the CSP or the user, which is introduced in any cloud production environment.

   c. Mandated adherence to the remote Access guidelines issued by DoT.

   d. **Processes and Procedures.**

      i. It should be mandatory for the CSPs to share their security governance processes and capabilities.

      ii. CSPs should be mandated to regularly update and publish their information security processes and procedures and Governance, Risk Management and Compliance processes. Should be mandated to be reviewed every quarter.

      iii. Mandatory provisioning of information about any breach of security in any domain, viz physical, Network, systems and applications.

[7] http://www.cloudsecurityalliance.org/guidance/csaguide.v3.0.pdf

iv. Mandatory Compliance to a process driven Change Management before implementation of any change in the cloud environment.

v. Mandated declaration, by the CSP, of the RA process for the technical support of the cloud infrastructure.

vi. Mandatory for the CSPs to ensure that their systems are updated with the latest OS patches and security software updates.

e. **Certifications.**

i. **Singapore's MTCS Certification Scheme[8].** With the objective of encouraging adoption of sound risk management and security practices by CSPs through certification, Singapore has established the Multi-Tier Cloud Security (MTCS) standard for Cloud Service Providers (CSPs). This cloud security standard covers multiple tiers of cloud security and the certification of the CSP is carried out by accredited third-party Certification Bodies. MTCS is only a certification regime which promotes guidelines for the CSPs on a host of issues like Cloud Outage Incident Response, Alignment of MTCS to Healthcare IT Security Policy & Standards, Harmonization of MTCS SS with IS0 27018:2014, MTCS to ISO 27001:2013 Cross Certification, ISO 27001:2005 to MTCS Cross Certification, MTCS to CSA STAR Cross Certification, CSA STAR to MTCS Cross Certification. The aim of the scheme is to ensure light touch regulation while providing assurance about the credentials of the CSP to the subscribers of services of the CSPs.

ii. **A similar certification regime, that has international as well as any India specific certifications, needs to be established for self accrediting of the CSPs for instilling confidence amongst the cloud services subscribers.**

f. **User SLAs offered.**

i. The CSP should be mandated to demonstrate its risk based management processes for control of information security.

ii. Mandatory provisioning of Root Cause Analysis of any failure within 24hrs of occurrence of the failure event.

iii. If the CSP is subscribing / outsourcing any activity(ies) to a third party, the CSP should be mandated to share their security related contractual obligations with the third party vendor.

iv. Mandatory provisioning of activity logs for audit purposes.

v. Data to be used only for the purpose for which it was collected. Any unauthorised use, even for extraction of high level business intelligence, should be prohibited.

5. **Promulgation of laws, regulations and other mandates.**

a. Data protection and privacy requirements should be mandated by governing laws. For ensuring privacy of personal data and the security of information and computer systems the CSPs should agree to subject themselves to the Indian Laws, regulations and other mandates for investigations into any breach of security.

[8] https://www.ida.gov.sg/Programmes-Partnership/Store/MTCS-Certification-Scheme

b. In order to protect personal data from loss, misuse or alteration, many countries like Japan, New Zealand, Australia and those of the Asia pacific Region and others have adopted data protection laws that require the data controller to adopt reasonable technical, physical and administrative measures, based on the privacy and Security Guidelines of the Organization for Economic Cooperation and Development (OECD) and the Asia Pacific Economic Cooperation (APEC) privacy framework. Even in Europe the European Economic Area (EEA) member states have enacted data protection laws that follow the principle set forth in the 1995 EU data protection directive abd 2002 ePrivacy Directives (as amended in 2009).

Our Recommendation

6. Customer is the best judge for understanding his business's requirements for security and compliance and hence the customer should select the appropriate cloud service model that provides the desired security controls. Service providers enable and offer different service models and customers should pick up a model that meets the regulatory and compliance model based on their business model. In view of the above, **from a regulatory perspective, a self certification regime, that has international as well as any India specific certifications, needs to be established for self accrediting of the CSPs for instilling confidence amongst the cloud services subscribers.**

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

Our Response

1. In line with the requirement of protection of data, it is imperative that the data user should be assured of complete deletion of all his data and any traces thereof, once the user decides to terminate the services of the CSP and exits out of his Data Center. Therefore, it is important that the exit or termination clause is transparently decided upon upfront, during the process of requisitioning of the services itself and is legalized in their SLA and contract. Once the termination clause is executed, for ensuring the security and privacy of the user's data, the user has the "right to be forgotten" and the CSP is obligated to ensure that the user's data is wiped out from all the storage and backup systems of the CSP. Accordingly, following termination or exit provisions may be defined for ensuring security of data or information over cloud.

   a. The CSP should be mandated to provide necessary handholding and transition support to ensure the continuity and performance of the Services to the complete satisfaction of the user, at the end of the contract period or upon termination of contract.

   b. Tentative Costs, if any, for the exit / migration process should be informed to the customer, at the beginning of the services itself.

   c. On execution of the exit / migration clause of the agreement, first and foremost the user's data should be handover to him in an open readable format which is acceptable for use.

   d. Post due verification and approval from the customer, the process for deletion of the customer's data should be initiated by the CSP.

e. It is the responsibility of the CSP to permanently delete all the customer related data, including the backups, as per the signed agreement.

f. In case retention of any data or its representation in logs or any other format is mandated from CSPs jurisdictional regulatory perspective, the same should be informed to the customer.

g. The CSP should be obligated to inform the customer about the completion of the mandated period of CSPs jurisdictional regulated retention and subsequently about the complete deletion of the retained data.

h. The CSP should be mandatorily obligated to ensure that the VM related data of the customer's VMs, collected during routine VM introspections, is not shared with any other customer with or without any monetary consideration.

i. The customer too should be obligated not to disclose any of the technical expertise / operational models / any other operational details of the CSP's cloud services setup to any of it's competition.

j. The confirmation for completion of all activities, especially the assurance that all the customer's data has been permanently deleted from the servers, storage and backup systems of the CSP, should be mandated to be provided in writing to the customer by the CSP.

k. CSP should be mandated to ensure that the data cannot be forensically recovered.

l. It should be obligatory on part of the CSP that the activities, pertaining to the exit management of the customer from the CSP's cloud setup, should in no way hinder the continuance of the customer's services.

m. In case of a CSP winding up his business, the CSP should be responsible for all activities required to train and transfer the knowledge to the Replacement Agency (or CSP) to ensure continuity of services of the customer.

n. The CSP should be mandated to ensure that all the documentation including policies, procedures, asset registers, configuration documents, Sign-off document, Maintenance Manuals, Administration Manual, Security Manual and others (if any) as per acceptable standards, Installation and maintenance manuals and other hardware Trouble Shooting Guide / Handbook for helpdesk which describes the various trouble shooting methods etc. are kept up to date and all such documentation is handed over to the customer during the exit management process.

2. **Migration from One CSP to Another.** Apart from the clauses suggested above, for ensuring smooth migration of the customer's setup following provisions are needed for live migration to cloud and for migration from one cloud service provider to another,

   a. CSP should be mandated to support the customer in migration of the VMs, data, content and any other assets to the new environment that the customer is migrating to.

   b. CSP should be obligated to support and assist the customer till he is able to successfully deploy and access the services from the new environment.

Our Recommendation

3. **A detailed exit clause elucidating the exact exit / migration process, especially for continuity of customer's services and specification of measurable metrics, should be mandated to be part of any agreement between the CSP and the customers[9].**

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

Our Response and Recommendations

1. As per the Cloud Security Alliance's (CSA) guide, security ownership in Cloud varies as per the Cloud Service Deployment models. For IaaS, service provider is responsible for physical security – data center and rack access, hypervisor level security. While for SaaS, service provider completely owns the security. The guide states that "for IaaS build security in and as you move up the layer build the security in the contract so that it is clearly defined and understood between service provider and customer". Additionally, it is the processes and procedures for ensuring security and the discipline of the people following those processes and procedures in each stakeholder's organizations, viz (a) the cloud service provider, (b) the application provider as well as (c) the user organization which determine the security of the cloud services. Accordingly, security of a cloud services can only be assured through cooperative and transparent sharing of responsibilities amongst all these stakeholders. Some of the responsibilities of each are tabulated below.

2. **Cloud Service Provider.**

   a. Adherence to security processes and procedures as listed in response to question no 10 above.

   b. Obtaining and maintaining certification of the services and security levels offered by the CSP.

   c. Ensuring data integrity and confidentiality.

   d. Ensuring clean deletion of data from older storage systems once they are being removed / replaced.

   e. Access to the data Centers through proper verification and by authorized persons only.

   f. Conduct of due police verification of each and every individual employed in the data center.

   g. Adherence to the security instructions, regulations and laws of the land / any agreements that bind the CSP to the laws of a distant land.

   h. Ensuring compliance of SLAs agreed with the user.

   i. Ensuring compliance of all CSPs obligations by the third party outsourcing partner.

[9] http://www.cloud-council.org/deliverables/CSCC-Security-for-Cloud-Computing-10-Steps-to-Ensure-Success.pdf

3. **Application Provider / B2B user.**

   a. Enactment of stringent SLAs with the CSP.

   b. Data preservation strategy and guidelines.

   c. Ensuring VAPT of the proprietary application being hosted in the cloud infrastructure.

   d. Building redundancies into its services.

   e. Ensuring confidentiality of information.

   f. Ensure no sharing of user's information to maintain his privacy.

   g. Obtaining and maintaining certification for the services and security levels offered.

4. **User.**

   a. The maturity, effectiveness and completeness of the risk adjusted security controls implemented by an organization, at different levels viz Physical Security, Network Security, System Security and Application Security including Information Security, determine the level of security that an organization is willing to accept.

   b. Subscription to the services for a disaster recovery at a different physical location and may be a different cloud service provider as well.

   c. The level of data resilience and redundancy opted for storage of data is solely dependent on type of service opted for.

   d. The user is completely responsible for the security and protection of data in the user's device.

   e. It is the users responsibility to ensure proper cyber hygiene for the user's devices and equipment.

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?

Our Response

1. The decision to move data from one jurisdiction to another is purely a business decision that a CSP would take primarily based on financial / ease of doing business considerations. In the current model of services provisioning through the clouds, mostly the location of service provisioning or the storage of user's data is totally opaque to the users spread across the globe. While subscribing to the CSPs services, even the users are either wilfully being oblivious to obtaining the information about the location of the CSPs setup or are not educated with impunity about the same by the CSP. Therefore, for ensuring that some credible customer support is provided by the CSPs, as an initial step, it is important that the governments across the globe synergise to enact international agreements and laws that are applicable across the globe in all the jurisdictions.

2. While the peculiar characteristic of the cloud based services such as the storage of data being ab-initio architectured to be stored in distributed, multiple locations provide for better survivability and security of the data, however, they also introduce challenges for implementation of the laws of the land. Since, multiple geographic locations are involved in utilization and provisioning of services and storage of data, **it is imperative that the laws for ensuring the security of the data, privacy of an individual and necessary disclosures to introduce transparency are also enacted as,**

   a. **Global level agreements which are bounden on all the stakeholders of the cloud computing services eco-system.**

   b. **Bilateral agreements, similar to those being enacted for exchange of monetary information for ensuring taxation compliances, can provide the necessary succour for the user's and clients in the eventuality of any violations that occur due to the movement of data across the borders into different jurisdictions.**

3. Examples

   a. On 15 Jul 16, in a judgement in a US appeals court, Microsoft was exonerated for refusing to give police user data stored overseas even when the data sought belonged to a drug trafficker. The court categorically told the police that "the Stored Communication Act (SCA) does not give US courts authority to force internet companies in the United States to seize customer email contents stored on foreign servers." Microsoft's case was being supported by the Information Technology and Innovation Foundation, a Washington-based tech policy think tank who opined that "data stored in other countries should be sought under auspices of a Mutual Legal Assistance Treaty designed to let police agencies around the world to help one another". As per an article[10] of The Channel News Asia, "the US has such mutual assistance treaties with more than 50 countries, including Ireland".

   b. In the European Union, cross border transfer of personal data of users within EU, is only permitted to be in the regions or States that have privacy and data protection laws matching EU standards[11]. In light of the reported bulk surveillance undertaken by US Law Enforcing Authorities and the European Court of Justice ruling it to be against EU's data protection laws, EU has had to review it's 'Safe Harbor agreement' with US. Though even the renewed version of this agreement, known as the 'Privacy Shield', has been criticized for not addressing the concerns of bulk surveillance practices completely, however, it has elucidated seven privacy principles to enable transfer of data among various jurisdictions. These principles bind the CSPs to necessarily,

      i. **Notice:** Inform customers about the collection of their data, its usage and how the user's can query / lodge complaints.

      ii. **Choice:** Provide customers the option for opting against (opting out) the collection, forwarding / transfer of the data to third parties.

      iii. **Accountability for Onward Transfer:** Transfer data to only those third parties that follow adequate data protection principles in conformity of the EU guidelines.

      iv. **Security:** Make all efforts for prevention of loss / theft of the collected information.

[10] http://www.channelnewsasia.com/news/business/microsoft-wins-appeal-to/2958542.html
[11] Article 25 of the 1995 Data Protection Directive of the European Union

v. **Data Integrity & Purpose Limitation:** Ensure that the collected data is relevant and reliable for desired purpose for which it is being collected.

vi. **Access:** Enable access and editing (correction / deletion / addition) of the customer's information by the customer himself.

vii. **Recourse, Enforcement & Liability:** Ensure enforcement of these rules.

4. **Indian Scenario.** Within India apart from the laws, acts and rules described in the consultation paper, the 'The Indian Contract Act, 1872', defined under Article 366(10) of the constitution, offers an alternative solution to protect data. According to this Act, the aggrieved party is entitled to receive compensation for any loss or damage caused to it whenever the loss is caused due to a breach of contract. Or the court may also direct "specific performance" of the contract, against the party in default, in exceptional cases. Hence, under this act the Indian companies / individuals may enter into contract with the CSPs. This act mandated contractual bindings and to a large extent fulfills the requirements of national legislations of overseas customer(s). Based on 'The Indian Contract Act, 1872', a host of Indian ITES services companies, especially those in the BPO / outsourcing industry, routinely incorporates international arbitration clause(s) for dispute resolution wherein the contracts may include,

   a. Arbitration rules of London Court of International Arbitration (LCIA), UNCITRAL, ICC (Paris), etc.

   b. The governing law under the Agreement(s) wherein any action arising hereunder is construed in accordance with and governed by the substantive and procedural laws of the customer's national laws without regard to the conflict of laws provisions thereof.

   c. Submission to the exclusive jurisdiction of customer's national courts and forums.

   d. Acceptance of mediation to resolve the dispute under the International Mediation Rules of the International Centre for Dispute Resolution of the American Arbitration Association ("ICDR").

5. Additionally, some Indian IT MNC companies that have a substantial offshore clientele have stipulated very stringent policies to ensure the protection of their client's information by contractually binding their employees for confidentiality. As part of their employment terms and conditions, the employees are liable to be charged in case of any negligent handling of data resulting in any kind of breach of security.

6. Therefore, in case of any violation of consumer data, while the same is being shifted from one jurisdiction to another, the client can be protected through internationally binding bilateral laws.

7. It is learnt that Indian privacy laws are as yet under formulation and hence it's difficult to benchmark the adequacy of privacy laws of other countries wherein the data of Indian citizens could be transferred by the CSPs. Accordingly, for facilitating formulation of a comprehensive guidelines for ensuring security of data when transferred from one jurisdiction to another, it is suggested that,

   a. Above mentioned seven principles of the 'Privacy Sheild' be considered for policy formulation.

   b. Users should be provisioned adequate customer care facilities for registration and redressal of complaints in their own home country in the eventuality of any misuse of their data across borders / in the foreign jurisdiction(s).

c. CSPs should be obligated to protect citizens' data from access by foreign intelligence services by inclusion of explicit clauses that prevents foreign intelligence agencies from accessing customers data.

Our Recommendations

8. **It is imperative that the laws for ensuring the security of the data, privacy of an individual and necessary disclosures to introduce transparency are also enacted as,**

   a. **Global level agreements which are bounden on all the stakeholders of the cloud computing services eco-system.**

   b. **Bilateral agreements, similar to those being enacted for exchange of monetary information for ensuring taxation compliances, can provide the necessary succour for the user's and clients in the eventuality of any violations that occur due to the movement of data across the borders into different jurisdictions.**

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?

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?

Our Response

1. In the present times when political volatility is prevalent across the globe, there is an urgent need for international cooperation in the fight against transnational crime and terrorism. In the cyber space, the need for such international level agreements gets further accentuated due to the internet's inherent ability to provide seamless access to distant locations sans any boundaries. Consequently, the operations of non-state armed groups, terrorists, and transnational criminal organizations are becoming global in scope. The ability of ISIS being able to recruit individuals for its nefarious activities, without being physically present in a location bears testimony to this.

2. Modern states need to developed mechanisms for requesting and obtaining evidence for criminal investigations and prosecutions. When evidence or other forms of legal assistance, such as witness statements or the service of documents, are needed from a foreign sovereign, states have the twin options of cooperating informally through their respective police agencies or, alternatively, resorting to what is typically referred to as requests for "Mutual Legal Assistance." The Mutual Legal Assistance Treaty(ies) (MLAT) is an agreement between two or more countries for the purpose of gathering and exchanging information in an effort to enforce public laws or criminal laws. The scope of this assistance may take the form of examining and identifying people, places and things, custodial transfers, and providing assistance with the immobilization of the instruments of criminal activity. It is brought out that India has MLAT agreements with 38 countries as listed on the CBI site[12]. Some other examples of multilateral MLATs are,

   a. Convention on Mutual Administrative Assistance in Tax Matters.

[12] http://cbi.nic.in/interpol/mlats.php

b. European Convention on Information on Foreign Law.

c. European Convention on Mutual Assistance in Criminal Matters.

d. European Convention on the International Validity of Criminal Judgments.

e. United Nations Convention against Transnational Organized Crime

3. MLATs apart, assistance may be denied by either country (according to agreement details) for political or security reasons, or if the criminal offence in question is not equally punishable in both countries. To obviate such situations, especially if the data hosting country is not inclined to India's interests, local hosting of servers and storage should be mandated for those SaaS providers. India is the fourth largest country in terms of Internet users in spite of having an Internet penetration of a measly 6.9%[13]. Therefore, India is in the envious position to be able to leverage its market size for making other jurisdictions to legislate similar laws to ensure the security and privacy of data of its citizens and also force the SaaS providers to host their applications in local data centers. The recent favourable verdict that Microsoft got in the case as mentioned above (The Channel News Asia article[14]) reinforces such a requirement. This article itself acknowledged the fact that "Microsoft's legal win came with the risk that foreign governments would begin forcing tech companies to rely on local servers to keep information away from US authorities, the ITIF warned".

Our Recommendations

4. **India should have maximum possible number of "Mutual Legal Assistance" agreements.**

5. **India should encourage local hosting of servers and applications.**

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 there under? Please comment with justification.

Our Response

1. **Applicability of Indian Telegraph Act, 1885 to Cloud Computing.** The CP at para 5.10 has stipulated that "*the cloud is a means to send and receive data operating by way of a closed network or the Internet. Therefore, a cloud service provider would be seen as establishing, maintaining and working telegraphs for the purposes of the Telegraph Act, under a license to be issued by the licensor.*" It is brought out that cloud computing infrastructures are merely for processing, storage, back up and retrieval of data. Even the classification of various cloud computing services deployment models for provisioning cloud computing services are as per the service that they provision i.e. IaaS, PaaS and SaaS and are in no way classified as per telecom services. Additionally, the other end of this communication channel is a user device which range from handsets to smart TVs to even the M2M devices. It is brought out that in case the cloud computing infrastructure is being construed to be under the ambit of Indian Telegraph Act 1885, then even the handsets, smart TVs and M2M devices too would be subjected to this act. Therefore, it is submitted that cloud computing should not be subjected to the Indian Telegraph Act 1885 and should be dealt with a light touch regulatory regime.

2. **Light Touch regulations.**

[13] http://royal.pingdom.com/2010/07/27/top-20-countries-on-the-internet/
[14] http://www.channelnewsasia.com/news/business/microsoft-wins-appeal-to/2958542.html

a. In India, following general and specific legislations, that must be necessarily complied with by the CSPs, prescribe various general, technical, financial, and security related conditions for the CSPs. Accordingly, it is submitted that a light touch regulatory regime that facilitates growth of CSPs while addressing national security concerns is most desirable.

i. Income Tax Act, 1961.

ii. Consumer Protection Act, 1986.

iii. Payment and Settlement Systems Act, 2007.

iv. Indian Copyright Act, 1957.

v. Central Excise Act, 1944.

vi. Prevention of Money Laundering Act, 2002.

vii. Information Technology Act, 2000.

viii. Foreign Exchange Management Act, 1999.

ix. Customs Act, 1962.

b. Cloud services means services made available to users on demand via the Internet from a cloud computing provider's servers as opposed to being provided from a company's own on-premises servers. This could be an organisation own shared service or be an outsourced CSP. There should not be any license or registration whatsoever for CSP, except the OTT services providers.

c. As of today IT service providers and IDCs are required to be registered under the Companies Act and are subject to a host of regulations including Shops and Estb. Act, MRTP, IT Act etc. The act that needs to be amended on an immediate basis is the IT Act as that is the most relevant to a data processor.

Our Recommendations

3. **Cloud computing should not be subjected to the Indian Telegraph Act 1885.**

4. **Cloud Computing should be dealt with a light touch regulatory regime with no requirement of licensing / registration.**

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.

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?

Our Response and Recommendations

1. For enhancing the adoption of cloud computing and creating an environment that is conducive for establishment of data centers in India it's imperative for the government / any policy maker

to provide a policy framework and an environment that shall promote improvement of existing as well as establishment of new infrastructure for accessing digital services, provide incentives and resources for innovation and promote confidence that using cloud services shall be secure and beneficial for the masses. A study conducted by OECD has found that (a) Development and Availability of Local content, (b) High Speed, High Availability Internet Infrastructure and (c) Affordable data Access prices are the three inter-related elements which feed into each other in a virtuous circle and must be adopted as the leads to formulate key lines of policy considerations.

a. **Development and Availability of Local content.**

i. Youth is the driving force for growth of internet as it provides them with instant knowledge as well as acts as a library that is available anywhere and all the time. Therefore, the government, especially the ministry of education, should leverage the cloud facilities for creating an enabling learning environment for improving basic literacy (e.g. drafting, language, etc), critical thinking ability, as well as media, information and digital literacy skills.

ii. Presently, even the basic service like banking and rail reservation (IRCTC website) through internet are usable by only the English speaking population. It is imperative that content development, especially in local vernacular, should be encouraged. As a policy it is recommended that **the government can provide incentives for startup ventures who provide their content in at least 3 to 5 Indian languages.**

iii. ICT equipment such as computers, mobile phones, cameras, scanners and audio / video recorders are important tools for digital content creators. Though the governments' 'Make in India' initiative shall give an impetus to easy availability of these basic tools for content creation, but other measures like removing any trade barriers, taxes or levies that limit the development, production and importation of these devices, should also be considered.

b. **High Speed, High Availability Internet Infrastructure.**

i. It is suggested that an important area for the governments' focus should be to be an enabler for increasing international Internet connectivity with India. Given our geographical location, India is aptly located to be the global hosting center. **Steps that lower the costs and barriers of delivering international bandwidth are particularly important.**

ii. In some cases the marginal cost of extending a backhaul connection to an additional location / community could be much lower than the benefit it could potentially provide. It is suggested that any government investment in road construction or electrification should consider installing the infrastructure for OFC networks at the same time to save on the significant digging costs. These backhaul networks can support both fixed and mobile Internet connectivity over the last mile.

iii. **Exemption of 'Right of Way' (ROW) charges for laying optical fibre.** According to the "State of Internet" Report by Akamai, India's average broadband speed is less than the half of the global average & peak speeds. The ROW charges for laying Optical fiber is very high in Metros & Tier 2 Cities where the generation & hosting of the content will be highest which makes it very difficult to provide high speed Internet to broadband users. **Exempting ROW for rolling out the fibre network to provide**

high speed broadband services shall entice global content owners to move the content in the country for better accessibility & at affordable cost.

iv. **In-building Solutions.** Availability of seamless and ubiquitous connectivity using a single and (or) multiple devices, while being stationary or on the move, outside a building or within a building has become a necessity. Selective availability of wireless / wired connectivity to the residents / visitors to a building due to exclusive agreements between the premise owners and a single or limited number of service providers is a highly discriminatory and anti-competitive practice and needs to be curbed for better adoption of cloud computing services. Therefore, it is recommended that **free and neutral access to all Multitenant Campuses, Buildings, Apartments and other buildings should be mandated.**

v. **Local Hosting of Content.** Latency (delay) in availability of the internet based content plays an important part in the kind of experience a user has while accessing the same. Local hosting helps in development, deployment and availability of more advanced services which require low latency connections, such as multi-media streaming, gamming applications, VoIP, etc. It also acts as a catalyst in ensuring faster and greater adoption of net based services. To this end, **local hosting of content ensures that the ISPs prefer to route the traffic locally thereby reducing response time from a few seconds to a few milliseconds resulting in better user experience of services utilization over the internet.**

c. **Affordable Data Access prices.** Formulation of policies that promote affordability of data services is a must in India where the per capita income is still languishing at around $1500. Though Indian telcos had introduced innovative pricing for data services for enhancing the affordability of data services, however, the same has been prohibited through the introduction of discriminatory pricing regulation.

2. Certain other measures that shall aid in ensuring establishment of data centers and fast paced adoption of cloud computing setups based services are as given below.

   a. **Subsidize power for development of domestic content hosting services.** Industrial Power rates vary from State to state. In an Internet Data Centre, Power is the most critical cost element which due to its high costs makes hosting of content unviable in India as compare to developed countries across the Globe. Concerted efforts at providing power subsidy to Internet Data Centers will help transfer the benefits for hosting services facilities thus making it lucrative for them to Invest in India. As per the Data Centre Risk Index Report by Index, Hurleyplamerflatt& Cushman & Wakefield, Power Security still remains a significant risk which puts India on rank 25 among the Top 30 destinations in the Globe.

   b. **Tax holidays for content provider hosted in Indian data centers.** The government should look at providing Tax holidays for the companies that deliver digital content or services through Servers based in India. Policies for establishing Data Centers in special zones, like the STPs, shall go a long way in attracting content hosting in India. It would helps companies draw long term commitment in terms of choosing India as the preferred location for Hosting & delivering digital content. E.g. In US Virgin Islands, companies can save up to 90% on their Federal & State Taxes that too for a period of 15 years. Certain other countries which offer such tax benefits are Switzerland, Ireland, Singapore etc.

3. **Promoting establishment of data centres in India.** From the Capex perspective, Content Hosting Services costs are on account of (a) Real Estate i.e space for developing a Data

Center, (b) Power for IT systems and environmental conditioning purposes and (c) Physical Security of the IT systems such as Servers, Storage and networking equipment. It is the relatively higher costs of the first two components of Capex that has prevented evolution of attractive business case(s) for the international / domestic community to establish data centers and host content in India.

4. From the regulatory perspective, as a first step towards creation of an environment conducive for cloud hosting, it is imperative that the existing regulations and guidelines for the telecom sector too are revisited, especially those that regulate the (a) Cable Landings, (b) IPLCs, (c) DLCs, (d) interconnects and terminations, (e) strength of encryption capabilities, (f) broadband QoS, (g) power grid supply and (h) green policy, (j) spectrum quality and (k) availability and to some extent even the (l) spectrum costing. Given India's geographic positioning, it is ideally located to be the natural choice for establishment of a transit hub for cable landings and consequently global data exchange points. However, it's disappointing to note that the Asia Cloud Computing Association's (ACCA) Cloud Readiness Index 2016, has rated India second last in its parameter for international connectivity (Refer Table 3 below). Simple realignment / tweaking of the existing regulations and guidelines, to make Indian shores more competitive for data hosting, have the potential to contribute towards making India an attractive destination for cloud hosting services.

Rank, Country	CRI#01 International Connectivity	CRI#02 Broadband Quality	CRI#03 Power Grid, Green Policy, and Sustainability	CRI#04 Data Centre Risk	CRI#05 Cybersecurity	CRI#06 Privacy	CRI#07 Government Regulatory Environment and Usage	CRI#08 Intellectual Property Protection	CRI#09 Business Sophistication	CRI#10 Freedom of Information	TOTAL CRI 2016 SCORE	Rank Change
#1 Hong Kong	8.1	9.1	6.7	8.0	6.2	9.5	7.2	8.6	7.4	7.2	**78.1**	+4
#2 Singapore	6.4	9.4	6.5	7.8	6.8	9.0	8.6	8.9	7.3	6.0	**76.7**	+2
#3 New Zealand	4.6	8.2	7.6	6.8	7.4	9.0	8.1	8.7	6.9	7.2	**74.4**	-1
#4 Australia	4.3	8.0	6.6	6.3	7.6	9.5	7.4	8.3	6.7	8.3	**73.2**	-1
#5 Japan	3.9	8.9	6.7	5.9	7.1	8.0	7.8	8.7	8.3	7.8	**73.0**	-4
#6 Taiwan	4.1	8.8	6.7	6.4	7.0	9.5	6.7	7.4	7.1	7.2	**71.1**	+1
#7 South Korea	3.8	9.0	6.3	6.2	7.1	9.0	7.0	6.0	6.9	6.7	**68.0**	-1
#8 Malaysia	3.3	7.6	5.4	5.9	7.6	8.0	7.4	7.7	7.6	5.8	**66.3**	-
#9 Philippines	3.3	5.5	6.0	3.5	3.5	7.5	5.5	5.6	6.1	7.3	**53.8**	+1
#10 Thailand	3.8	8.6	6.0	5.2	4.1	5.0	5.1	4.6	6.3	3.8	**52.6**	-1
#11 Indonesia	1.8	6.3	5.4	2.7	4.7	6.0	5.6	6.1	6.1	5.8	**50.6**	+1
#12 India	1.7	5.6	5.1	1.9	7.1	4.5	5.5	6.0	6.0	5.8	**49.1**	+1
#13 China	1.6	6.6	5.3	2.5	4.4	5.5	6.2	5.7	6.1	1.3	**45.4**	-2
#14 Vietnam	3.0	6.7	5.4	2.6	3.2	5.0	5.4	5.1	5.1	2.4	**44.0**	-

Table 3: Showing the Cloud Readiness Index
Sources: Asia Cloud Computing Association report "Cloud Readiness Index 2016'

5. Para 2.2 clause (vii) of the ISP license states that *"Individuals/ Groups/ Organizations are permitted to use encryption up to 40 bit key length in the symmetric key algorithms or its*

equivalent in other algorithms without obtaining permission from the Licensor. However, if encryption equipments higher than this limit are to be deployed, individuals / groups / organizations shall obtain prior written permission of the Licensor and deposit the decryption key, split into two parts, with the Licensor." Imposition of such archaic restrictions when most of the world has moved to AES / DES with 128 / 256 bits or the more contemporary RAS with 1024 bits encryption algorithms tends to dissuade establishment of data centers in India and should be revised to bring them in tune with international norms.

6. **Encouraging business and private organizations utilize cloud services.** Coupled to solving the above mentioned impediments, enactment of laws that make the businesses feel secure about their data and privacy would go a long way in encouraging them for adoption of cloud based services.
7. Embracing Cloud services for government projects such as smart cities and e-governance.
8. Increase in carbon credits can be leveraged to incentivize SMB and enterprise segments.

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?

Our Response and Recommendations

Yes, there should be a dedicated cloud for government applications which should support a multi-tenant environment for the government applications only.

1. Government services are provisioned for and are requisitioned by all the citizens of a country. This is important to ensure,
   a. Better and optimised administration of the setup.
   b. Better database optimization.
   c. Better utilization of the resources as idle resources can be deployed for supporting services that might be facing peak loading. E.g. the Income Tax department's application is loaded during the income tax filing period. Therefore, some servers that are normally dedicated for processing PAN card applications can be redeployed and utilized for supporting the IT filing setup.
2. Given the country wide scale of utilization of the services, all the characteristics of clouds viz, economies of scale, multi-tenant setup, high level of security, etc can be exploited even if multiple applications of the government are hosted in single cloud setup.
3. Just as there is an exclusive network for provisioning essential services like water and electricity to all the citizens of the country, similarly, **the provisioning of government services through the cloud would be akin to essential services and hence, should be from an exclusive, open standards based, cloud setup hosting only the governmental services.**
4. **The cloud setup established for provisioning government services can be hosted in the government data centers or can be hired from private operators. Even if the setup is hired from private parties, hosting of only government services should be mandated, within that setup.**
5. **The setup should be mandated to be highly robust by provisioning multiple levels of redundancies, high grade resilience and near real-time disaster recovery capabilities.**

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?

Our Response and Recommendations

1. Rcom has been a Build and Operate and only operate vendor for some of the State Data Centers (SDCs) in India. Given our experience, the infrastructure and operational challenges face towards development and deployment of state data centres in India are as follows,

   a. **L1 Bidder.** The vendor for establishment of the SDC is selected through the bidding process wherein the selection is based purely on Least Cost or L1 basis. It is brought out that often the selected L1 vendor is a Network establishment vendor and does not have much expertise in establishing a Data Center (DC). This results in establishment of a sub optimised DC which falls short on performance as well. **Data Center being a specialised establishment, it is imperative that the primary selection criteria of the vendor for building the DC should be more on technological expertise and operational competence rather than commercial considerations.**

   b. **IT and Non IT equipment and operations bids to be separate.** Just as DCs have specialised IT requirements, so is the case with its non IT support setup. Each requires a specialist to implement the project. Quite often either the IT or the non IT lead becomes the System Integrator leading to compromised establishment of one of the setup and therefore it is suggested that the **tenders for IT and Non IT requirements should be two separate tenders instead of a single tender**.

   c. **Retrofitted Building.** It is brought out that often an existing office building is retrofitted to operate as a SDC. Normally, a DC building has greater floor strength than an office building. Therefore, the retrofitted building is not suitable for establishment of the DC and is often required to be shifted to another building. E.g. Manipur State DC has been established on the fourth floor of an office ware housing kind of a building. The building has no lifts for carrying of the machines nor does it have basic amenities like availability of water, etc. It is therefore suggested that the **SDCs should be viewed as an essential infrastructure for the state and should be housed in a separate specially build building rather than retrofitting an existing office building.**

   d. **Lack of Disaster Recovery Planning.** It has been observed that SDCs are planned as a standalone DCs without any credible Disaster Recovery (DR) planning. Since each state has a SDC, it is suggested that,

      i. **The SDC of an adjacent state should be nominated to be the DR DC for a state.**

      ii. **The nomination of DR should be on a round robin basis instead of reciprocal basis.** E.g Bihar should have a DR in Jharkhand, Jharkhand in West Bengal and West Bengal in Orrisa and Orrisa in Bihar.

      iii. **At least 25% of the SDCs capacity should be catered for the DR of the other states SDC.**

   e. **Lack of Farsightedness - Mismatch between the Consultants Design and Operational Requirements.** It has been observed that the SDCs have fallen short in terms of performance / resources / have a rigid architecture that does not support expansion / enhancement of services capabilities. This leads to wasteful expenditures on

account of additional hardware purchases negating the very elastic characteristic that a DC is required to have inherently. It is therefore suggested that **SDCs should be designed with due modularity and expansion capability built into them.**

f. **Continuity of Services.** SDCs often fall short in terms of availability of IT trained skilled manpower due to either lack of availability in that area / region and sudden change of operational contract. Therefore, it is suggested that,

   i. The **state government, as part of the Skill Development program, should appoint at least 30% of apprentices, over and above the basic manpower requirement of the DC.** This shall have the twin benefit of skilling the local youth as well as create bench strength for the manpower of the DC.

   ii. **At the end of the 3rd year of the operational contract of the existing vendor, the tender for continuing operations at the end of 5 years** i.e. end of the contract of the existing vendor, should be floated and the selection process should be complete by the end of the fourth year. In case a new vendor is selected for continuing operations at the end of the 5th year of operation of the existing vendor, then, the newly selected vendor should be mandated to provide at least 25% of the manpower as shadow manpower for understanding the DC operations and ensuring a smooth and seamless transition from one vendor to the other.

9. **Security concerns while provisioning L3 maintenance support from locations outside India.**