Cloud Computing Innovation Council of India Comments to TRAI’s Consultation Paper On Cloud Computing

Executive Summary | Summary of Recommendations

TRAI’s consultation paper on Cloud Computing presents valuable information and important questions, thoughtfully aggregated from industry analysis and observation of other government policy documents. It has raised several important prioritised issues about :

- Security & privacy,
- Interoperability & migration across cloud service providers,
- Escalations / complaints resolution & exit / termination criteria,
- Competition policy & cross-border cooperation.

Government policymakers in India and around the world are depending on innovations and orchestration from Cloud service providers and other ecosystem players to address these. A task force of technical and business experts within CCICI has deliberated over these during the last few months keeping the perspectives of both cloud user organizations as well as cloud service providers in mind. This document is a compilation of a vendor neutral, technology driven, “India first” perspective from the task force. Following is a summary of the recommendations :

- It is very important to specify an SLA/metrics framework that enables the cloud customers to map their business and technical–requirements–against the CSP’s offerings and make effective choices in an objective, repeatable and rational manner.
- Interoperability standards are currently at an early stage of evolution in the cloud industry. However from an India perspective, interoperability and easy migration between CSP’s is key to enabling adoption and deployment. Hence it is important that all CSPs be required to allow for easy export of customer data and applications in a commonly accepted standard that enables them to migrate the same into another CSP at will. Additionally, CCICI strongly recommends that TRAI should mobilise the setting up of an “OPEN” Interoperability test bed across the country with active participation from CSPs, cloud user organizations, industry and academia.
- Data and content privacy is a primary concern in moving to cloud. It is therefore important to quickly specify standards that can form the basis of contracts with CSPs. There are several such standards being proposed globally (eg.ISO 27018) and these.
- For certain domains e.g. Government, Banking or Healthcare, a risk-based, agile cloud procurement environment with continuous improvement adapting to shifting risk priorities should be encouraged by the Government (e.g. MTCS specified by Singapore govt.). This will enable proliferation of trusted cloud services ensuring :
  - Security of operation,
  - Data protection and privacy,
  - Compliance with local requirements and
  - Transparency.
- Dedicated cloud for government application & services (adhering to interoperability requirements) seems to be the most logical option considering current government initiatives. This would enable a leapfrog to embrace the benefits of this disruptive technology and competitive participation of multiple vendors without compromising security requirements. A framework for India specific certifications, needs to be established for (self)accreditation of the CSPs.

- The government should promote CSPs to provide **Citizen computing** (through public cloud and freemium models). This will open up a new world of innovative services and generate employment for the young educated Indians.
- Free and open Cloud APIs should be encouraged and published to enable rapid development of innovative and basic Cloud Services. Open forums should be encouraged to enable this.
- Integration of Cloud Computing with IoT (Internet of Things) is ultimately the need of the hour to enable rapid transformation of India to a digital economy. Innovation and research in these areas should be promoted.
- While encouraging the use of cloud services in the country, it is important to ensure that there are regulations in place that clarify the principles that should be followed by CSPs while shifting the data of their users from one jurisdiction to another. It is also important to understand the vulnerabilities of allowing data to reside in another country. Suitable policies need to be put in place to protect the country's interests.
- With the increasing use of cloud and huge amounts of data being generated in India, government should encourage local hosting. This would automatically address the quality of service as well as reduce security vulnerabilities
- The consultation should be expand to include "socially relevant" questions such as:

1. How can cloud computing bring enhanced access to technical resources for learning and "citizen computing" to all of our people, regardless of ability to pay?
2. How can cloud infrastructure leap out of the data center into the cheapest and most accessible hardware to which citizens have access, so that everyone can join "the Cloud" as they can attach their phones to the Net?
3. How can free software in the cloud enable young people to be more than users of platforms, and become instead skilled builders, using the resources commonly available in the cloud to make their livings improving the lives of people and businesses around them?

- It is perfectly right for TRAI to consider, as this paper does, the role of government in enabling CLoud Computing adoption and regulating market participants offering digital services. But something even more important will be lost if TRAI does not also consider these technological disruptions from the vantage of the social architect, understanding how these new technical materials can be used to improve the lives of ordinary people, and the intellectual development of Indian society. It may be appropriate to consider a dedicated initiative on "Societal Computing".

Detailed comments on the questions posed by TRAI are given in the following pages.

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 household utilities like electricity, water, telephone services, when we turn off the usage of the cloud computing resources, the same are made available for use by others. This further , can be compared with SaaS' pay-per-use model. One of the main reason for confusion on how to consume cloud services is synonymous to situation when household is trying to take electricity directly from the grid (/household interacting directing with electricity producers) PaaS and SaaS offerings have to mature to improve the utilization of cloud.
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. 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

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

			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

3. 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.**

Se r	**Requirement**	**Time to Market Support**	
No		**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. Easy availability of SDK environments and Open source communities around them can be exploited for speedy application development. 4. Customers can compare	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.

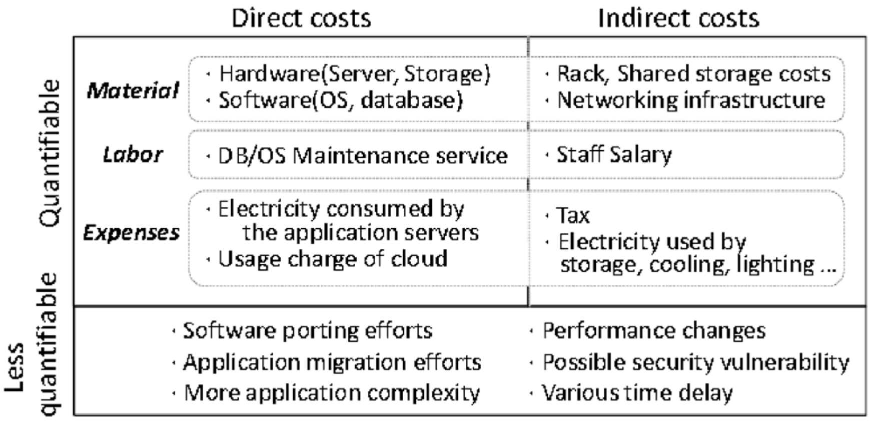
		ROI across each model of Cloud Computing – private/public/hybrid and decide the most optimal one for their cloud scenario.	
3	Promotion of Social Networking	1. Services are Always On and available Anywhere and Anytime on the device of the users choice. 2. Elastic Resource availability ensures that the 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. Integration of cloud service with other technologies like mobile will increase outreach, increased transparency and sharing of useful data via cloud based services will increase participatory governance. Government agencies can set up up cloud based data marts for data sets that may useful in the public domain. 5. Availability of localized content for application will help promote Social Networking, Participative Governance and E-commerce in all regions of the country (rural or urban)	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.
4	Participative Governance		
5	E-commerce		
6	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. Cloud services will also help end-user organizations implement highly cost effective services like DR and HA. Even SMEs, for whom such capabilities are cost prohibitive, can make use of them – on demand – using CSPs that provide such services. 4. DevOps is an upcoming model where cloud based services can be rapidly deployed and trialed at minimum risk. This convergence of IT and support leads to a unique sandbox which can push technology and user experience to new levels.	

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



		Direct costs	Indirect costs
Quantifiable	*Material*	· Hardware(Server, Storage) · Software(OS, database)	· Rack, Shared storage costs · Networking infrastructure
	Labor	· DB/OS Maintenance service	· Staff Salary
	Expenses	· Electricity consumed by the application servers · Usage charge of cloud	· Tax · Electricity used by storage, cooling, lighting ...
Less quantifiable		· Software porting efforts · Application migration efforts · More application complexity	· Performance changes · Possible security vulnerability · Various time delay

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 ChulTak, Bhuvan Urgaonkar and Anand Sivasubramaniam

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.

2. 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).

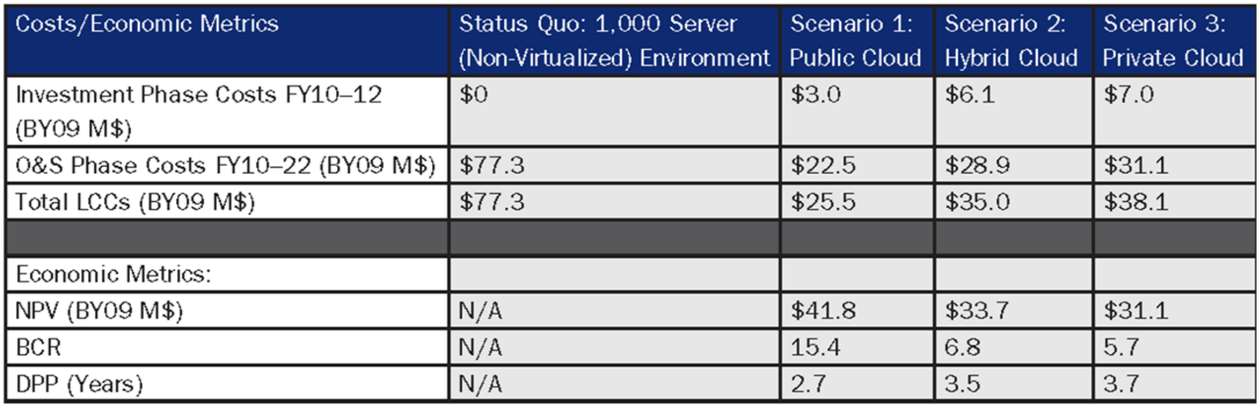
    b. Customer Set Duty Cycles (λ,f).

    c. Relative Duty Cycle Displacement (t).

    d. Customer Set Load (L).

3. 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.

4. The economic results of a 2009 Booz Allen Hamilton(BAH)[2]study (summarised at the bottom portion of the Table 1) clearly show that the projected **Net Present Value (NPV)** and **Benefit-to-cost ratio (BCR)** for different cloud implementation models are significant relative to the traditional IT setup environment. As per the study, the **Discounted Payback Period (DPP)** reflected the number of years it would take for each model's accumulated annual benefits to equal its total investment costs. 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.



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 Booz Allen Hamilton Study on economics of cloud Computing

Source: Booz Allen Hamilton Study on economics of cloud Computing[1]

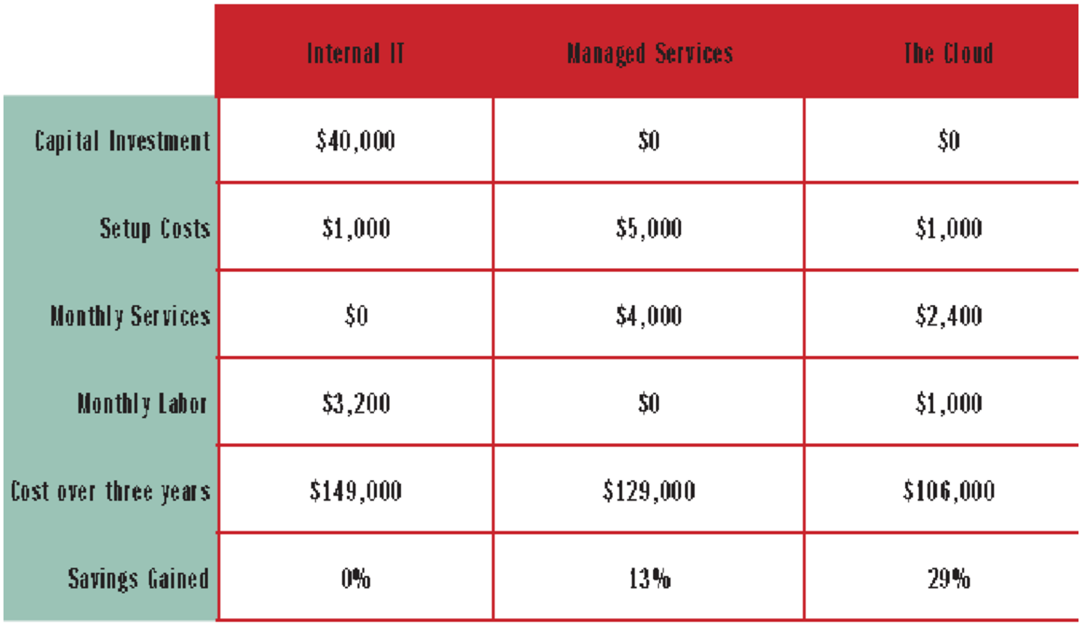
5. The "Cloudonomics: The Economics of Cloud Computing' from Diversity and rackspace hosting study contends that, "*There are many reasons for organizations to move from traditional IT infrastructure to Cloud Computing. One of the most cited benefits is the economics of the Cloud. Yet while many people 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

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

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 two application servers, two database servers and a load balancer across internal, managed and 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."*

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

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

<u>**Our Conclusions**</u>

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

   a. **Directly - through reduced costs.**

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

7. **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 compelling than any cost savings possible. Each type of Cloud computing model provides its own strong benefits and economic incentives. 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.** Ubiquitous Broad Band Connectivity with guaranteed performance at a reasonable cost will be a key factor in end user organizations adopting cloud computing services for business use.

   b. **Security and Authentication**

      i. **Physical Infrastructure and Compliances.** A well secured cloud computing hosting facility complying to international security standards such as ISO 27001 & ISO 27018 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.

      iii. **Availability of Multi-modal authentication mechanisms** for different types of users and user communities (application end-users, IT administrators, developers etc.)are also a critical factor in organizations selecting the type of cloud deployment model that suits their organization the best.

   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. One of the main concerns for enterprises that consider adoption of cloud computing is performance. 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.** End user organizations may consider the multi-tenancy of the environment at multiple cloud layers in their decision making process. At the IaaS layer, most CSPs provide an OS environment that is hosted in Virtual Machines that typically are multi-tenanted on one or more physical servers. This may or may not be issue for an organization based on the type of VM or VLAN segregation technologies used by the CSPs. At the PaaS layer, resources like Databases, Application Servers etc may be multi-tenanted and the customer will need to consider this in their decision making process. Finally, at the SaaS layer, the multi-tenancy is generally built into the application. E.g. an HR service provider in the cloud may service many customer organizations using the same hosted application. Therefore, cloud customers and end-users will need to consider their multi-tenancy requirements at each level before deciding on the type of cloud deployment model.

e. **Hybrid and Integration with existing on-premise services.** This is an important factor for many new cloud customers since the need to protect their existing IT investment is a major requirement. CSPs that provide easy mechanisms for **Application Integration** along with Manageability Integration will make it easy for customers to adopt their services. Customers will also find an easy migration path to utilizing more and more services from cloud, once their existing IT investment reaches end-of-cycle stage.

f. **Resiliency and Redundancy.** The kind of **High Availability** and **Disaster Recovery services** available from the CSPs can be a major deciding factor in customers when selecting an appropriate deployment model. A resilient and redundant infrastructure ensures robustness and translates into availability of services for the maximum up-time.

g. **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.

h. **Governance and Adherence to Regulatory requirements**. This is one of the most important factors in customers selecting their deployment model –especially for customers in certain sensitive domains like government agencies, banking etc. CSPs should be able to demonstrate transparently how their services at each level comply with the specific regulatory requirements relevant for the cloud customer’s business domain.

i. **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.

j. **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.

k. **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.

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

m. **Ease of use.** This an important factor in decision making considering multiple dimensions like Application Deployment Services, Application Management Services, Application Monitoring including Flexibility and Elasticity of Service Access and Requisition**.**

n. **Ease of Billing and Billing Verification.**

o. **Data Analytics Capability.**

p. **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.

q. **Geographic Boundaries and Co-Location.** In today's globalized economy, a cloud customer may have highly varied requirement as far as co-location and geographies are considered. It's very common to have large application providers in the cloud have their development, deployment and management organizations in one country while having their financial and billing services in another country and at the same time having most of their end-user base in two or three other countries or regions. In such an environment, the availability of cloud services from a particular CSP in multiple regions of the world become an important factor when deciding on the cloud deployment model.

r. **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

It is very important the cloud customers **carefully evaluate their requirements** for each of the above factors, **prioritize them appropriately and measure** each cloud deployment model or specific CSP against them so they can determine the right cloud computing model that they 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.**

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

Our Response

1. When one is migrating from one cloud service provider to another, we should first understand what is it that is migrating. If the solution deployed was a Infrastructure as a Service Solution, then the Migration is more of an equitable infrastructure setup in the new environment. It may seem simple in this case, however there may be issues with how data is being stored in different cloud environments. Understanding if the storage formats follow a specific standard and there are no data interoperability issues is a key concern in this case.
2. If we are looking at Platform as a Service or Software as a Service migrations from one cloud to another, then we have to essentially do a Software migration to a new Technical environment and the migration needs to be treated as a technical project, where skilled technical teams do a feasibility analysis and make recommendations for the actual migration .
3. The practices that seem to work well are around cloud service provider **viability, transparency, control and compliance**.
4. At a high level , issues related to switching providers include:
   - Retaining ownership of domain names.
   - Data portability.
   - Application portability, particularly in a PaaS scenario, and associated costs.
   - The cost of data migration to a different service, especially one with very different facilities for hosting important databases.
   - Portability of identity and access controls and associated costs. Many cloud service providers expect the customer to use the cloud service provider's identity and access control system. If the organization wants to move to a different provider, it might be forced to re-provision all those user accounts.
5. Organizations should also ask the cloud service provider about its policies and practices that affect the ownership, use, and retention of data (or related aggregated data and metadata) that is stored with the cloud service provider. In addition to that, when thinking about compliance obligations related to data stored and processed in the cloud, organizations should consider two issues. First, should the data in question actually be placed in the cloud, and what conditions would have to be met to do this? Second, what assistance can the cloud service provider provide to help the organization meet the applicable compliance obligations? To answer these questions, the organization must first understand what its own regulatory and internal policy requirements are. It is recommended that organizations develop a data classification policy and a set of —harmonized compliance requirements - a list that summarizes the organization's regulatory and internal policy obligations and that can, in turn, be used to define the requirements the organization has for the cloud service provider.
6. Finally, once an organization establishes the viability of storing and processing data in the cloud, it can address how to meet its regulatory compliance obligations as well as data privacy and security-related commitments it has made to customers, shareholders, employees, and other stakeholders. Just as important is the question of how it will show proof of compliance. The cloud service provider should clarify the processes and escalation paths it will follow in exceptional circumstances, such as notifying the organization in case of a data breach. The terms of agreement should therefore include a list of compliance-related documents that will be provided by the cloud service provider, including certifications, plans, and escalation paths.

7. A secure migration path is one of the most important factors to ensure seamless migration and deployment from one cloud to another. At the initial stage, it’s very important to consider and define the following so migration activities can be executed within a known framework:

   - **Define KPIS or SLAs for migration** clearly. Some applications are delay tolerant others are not based on the business scenario or customer environment.
   - **Define the appropriate type of migration** base on application or environment being migrated:
     - Offline vs. Real-time
     - With user involvement vs. opaque to the user
   - **Define the roles and capability requirements from each organization** involved in the migration – specifically the CSP and the cloud customer.

8. Once the overall framework, roles and responsibilities have been defined, it’s important to note that typical cloud migrations involve some steps that are manual and some that are automated via tools and scripts. Security requirements of the specific manual steps as well as tools and scripts being used , should be defined and implemented by the organization responsible for that aspect of the migration process.

   - Security of compute elements
     - Virtual Machines,
     - Pre-built application images,
     - License security
     - Others
   - Data and Storage security
     - At rest and during movement/migration
     - Along with context/state or without
   - Network path security
     - Authentication and trust mechanisms between end-points (source and target clouds)
     - Encrypted communication channels, protocols and secure messaging.
   - Secure migration of Identity and Authentication mechanisms

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

When dealing with cloud providers, government organizations must be sure that they own their data in order to maintain data and content privacy. That means organizations should explicitly be allowed to access any of their own data - including text, sound, video, or image files and software - for any reason at virtually any time. For leading cloud services, data ownership is certified by ISO/IEC 27018. We would recommend the Indian government considers relying on a code of practices such as ISO 27018 rather than developing a new regulatory framework to cover this concern. To be concrete, ISO 27018 requires that cloud service providers operate under six key principles:

1. **Consent:** CSPs must not use the personal data they receive for advertising and marketing unless expressly instructed to do so by the customer.
2. **Control:** Customers have explicit control of how their personal data is used
3. Transparency: CSPs must inform customers where their personal data resides and make clear commitments as to how that data is handled
4. **Accountability:** ISO/IEC 27018 asserts that any breach of information security should trigger a review by the service provider to determine if there was any loss, disclosure, or alteration of personal data
5. **Communication:** In case of a breach, CSPs should notify customers, and keep clear records of the incident and the response to it
6. **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 must subject itself to yearly third-party reviews.

It is recommended that CSPs get themselves certified against ISO/IEC 27018 which establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect Personally Identifiable Information (PII) in accordance with the privacy principles in ISO/IEC 29100 for the public cloud computing environment.

However, 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: customer's VM images, application images, databases, application level meta-data etc. This must cover not just online stores for such data, but also archival and any other off-line stores the CSP may be using for such types of customer data.

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

It may also be noted that international agencies are also looking at these issues and we expect 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:

- 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.

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.

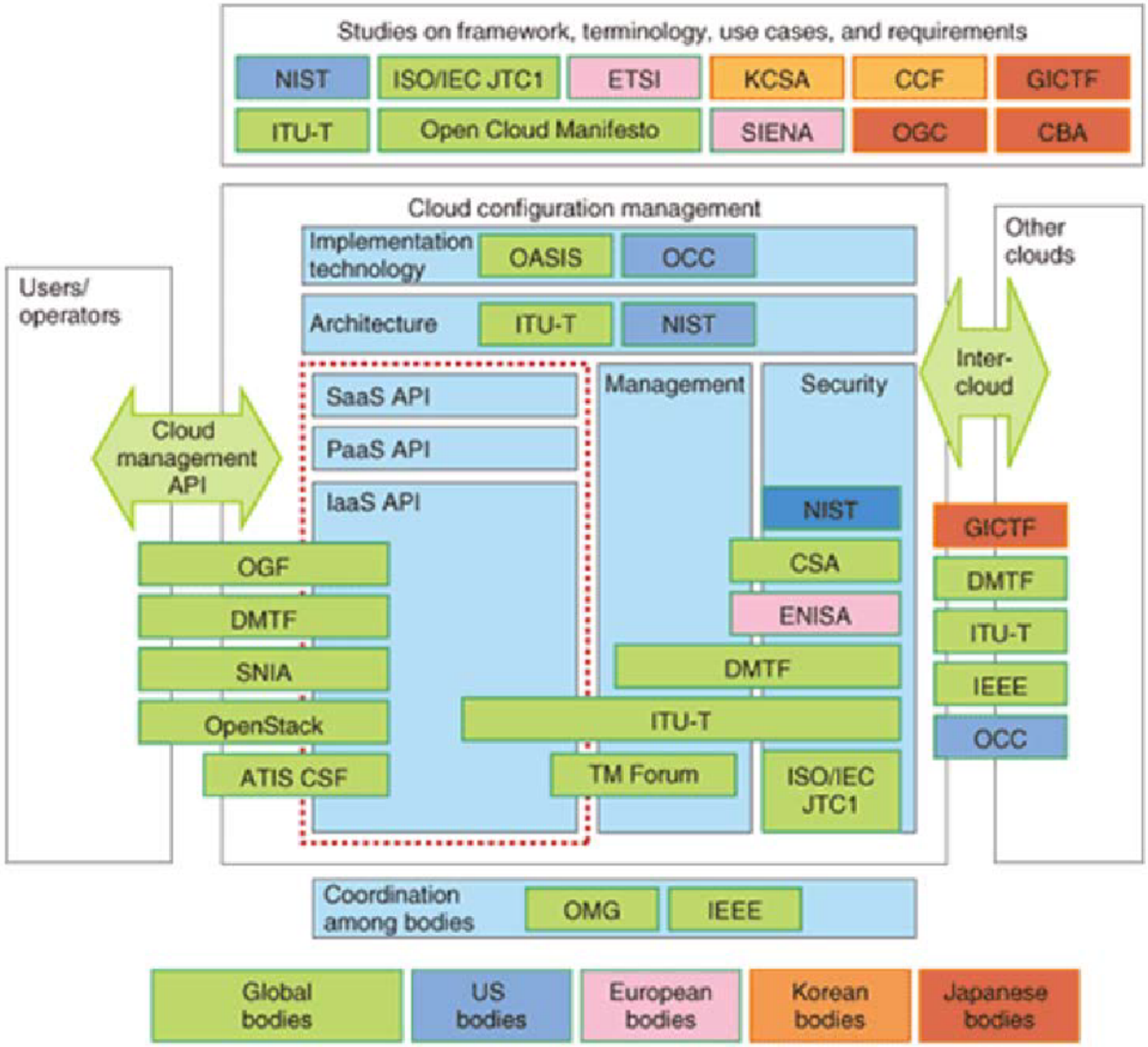
References :

http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=61498

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 Standards for Information Security Management ISO 27001 / ISO 27018 and Cloud Security Alliance framework to be the base for ensuring standardization across different cloud service providers.

CDMI for Data Storage . This single picture covers all standards (included in CCICI Whitepaper 2.0)



OGC: Open Government Cloud consortium
CBA: Cloud Business Alliance
SIENA: Standards and Interoperability for e-infrastructure Implementation initiative
KCSA: Korea Cloud Service Association
ATIS CSF: Alliance for Telecommunications Industry Solutions Cloud Services Forum

—Source: Standardisation activities for cloud computing, NTT, Japan. Reprinted with permission.

CSP must not introduce direct/indirect barriers for customer applications to interoperate, **they must also have the freedom and ability to innovate and create differentiation** from competitors to ensure successful business operations.

Interoperability standards are currently evolving in the cloud industry, though have been developed by various consortiums and associations , been in adoption in various countries , it is necessary to consider separate debate and consultation on regulatory framework and standards for the same at this stage. Since there is a need for interoperability, TRAI should fund an Interoperability Test Bed so that India can take the lead here. Or create public private partnership to initiate such initiatives and can help assess the commitment to "openness" of each CSP in the market as follows:

- Use Openstack as a baseline for Interoperability testing since it is emerging as a widely supported cloud API with support from many CSPs
- CSPs can be asked to show how they support the following between their cloud and Openstack:
    - Migration
    - Movement of Data
    - Interoperability in terms of abstraction, programming and orchestration
- Each CSP can be rated based on the level of interoperability they can demonstrate:
    - Support all requirements for migration, data movement and interoperability
    - Support all important requirements
    - Have a roadmap to support all important requirements
    - Have no plans to support important requirements
- CSPs can claim exemption for features and functionality in their clouds that are not available in OpenStack. Customers who use these features can then be made aware that they may be locked in to a vendor with specialized features and they can decide on using that based on their business scenario.

While measuring CSP's interoperability with OpenStack will be very useful to cloud end-users, Open Group recommends some additional points to consider when defining interoperability and operability at each layer:

- **Portability and interoperability of infrastructure components** are achieved by hardware and virtualization architectures. It is not important to consider from a cloud portability perspective.
- **For interoperability**, these elements should be considered: Application (including Management Apps) and Platform
- **For portability**, these elements should be considered: Data, Application and Platform

Interoperability of cloud services can also be considered from the online interoperability or offline interoperability perspectives. Online interoperability is crucial for applications operating in a multi-cloud environment (cloud services from multiple CSPs) and Offline interoperability refers more to data portability issues which have been discussed in other questions.

Going further into the requirements for online interoperability of applications, it is generally the customer's application components that need to interact with each other. As long applications use standard protocols and messaging/communication techniques and the CSP doesn't put in unreasonable barriers to their usage, the components should be able to communicate with each other across clouds without any explicit support from the CSP.

Beyond application level interoperability – specifically for inter-cloud management - CSP (cloud API level) API can be provided by implementing one or more of the following:

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

- **Deltacloud API**: Abstracts differences between clouds

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

Additional details and reference for the above APIs can be found at:
http://cloudtweaks.com/2013/10/importance-of-cloud-computing-interoperability/

Finally, CSPs must enable the following important capabilities to ensure interoperability between services:

- **Predefined & Published APIs - with protocols like JSON / XML or REST .** For API's reference implementations are provided and developed in consultation with industry bodies.
- Programming environment should be open (e.g.: Specifications for the language is available openly) .
- Orchestration should be tested in joint test-beds. Vertical integration points should be built on top of common test-bed , which uses common cloud underneath.
- Regulatory framework should include anti-competitive processes applicable to cloud service providers.
- Since , at present, it is not possible to mandate standards, since they are evolving. However, Govt. should try to assess the commitment to "openness" of different clouds as follows.
  - Openstack is emerging as a widely supported cloud API with support from many vendors.
  - Vendors could be asked to specify how they would support migration (Q4) movement of data (Q5) and interoperability (Q6) between their clouds and Openstack.
  - The different vendors could be rated on whether they (1) support all requirements for migration/data movement/interoperability (2) all important requirements (3) have a roadmap to support all important requirements (4) have no plan to support important requirements.
  - Vendors can claim exemption for functionality in their clouds that is not available in Openstack, if such functionality exists. Customers who use this functionality would then be aware that they may be locked in to a vendor.
  - Clarify that another motivation for interoperability is the ability to build cross-cloud applications which leverage specialized services from each cloud. This seems to be implied, but not spelled out.
  - The discussion seems to be centered around VMs. The drafts should include containers as well.
  - Interoperability is the ability to treat a collection of clouds as a single resource pool. In addition to common APIs, it implies cloud clustering software, unified management and monitoring, as well as some sort of brokerage - automatic translation of resource requests (e.g., if I want a tiny VM in Amazon terms, I should get the corresponding VM in Rackspace

without explicitly knowing what this corresponds to) as well as policy-based cloud selection. The definition of portability is correct.

- Since application migration is likely to be between same versions of OS, virtualization technology is unlikely to be a bottleneck. SDN/NFV is leading to some standardization in networking migration.

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

QoS in Clouds

In the cloud spectrum, QoS plays a key role in assuring the user on its expectation from cloud services. One of the significant features of the cloud model is that it moves the control of cloud resources, (be it IaaS, PaaS, or SaaS) from the user's domain to the provider's domain. As a result, what was earlier implicit to the design of the service, in terms of its behavior (with regards to its performance, availability, reliability, security, etc.) has to be specified explicitly when moved to the cloud.

Cloud services are often deployed to utilize idle resources and hence, are exposed to the constraints of sharing resources. For example, the virtualization technologies help different users in deploying multiple VMs on one physical host. This kind of scenario leads to the most prominent question—how a user application that is running on user's VM is impacted due to another VM co-hosted on the physical host? It is to be noted that criteria such as **performance interference, availability reduction, bandwidth issues, security vulnerability, and breaches are the determining factor for the impact.**

QoS needs to be definitely targeted for cloud platforms, particularly in scenarios like that of India, because of the expected scale of the problems. While a generic solution to address most QoS issues can be to increase the capacity of the data center or dedicated application provisioning, it may not always lead to an optimal or even reasonable solution. Instead, building services and platforms that address the issues of QoS can lead to cost effective and innovative solutions. Factoring in QoS requirements will enable quantification of user expectation. This quantification will enable providers to allow measurement and build autonomous methods for ensuring QoS. Quantification further helps in making this expectation uniformly visible across different layers of the cloud provisioning stack and improves preservation while moving across different providers.

The complete set of QoS parameters that can help measure CSPs comprehensively should include dynamic metrics as well as static metrics.

- Dynamic metrics typically include things related to performance and speed of operations, latency etc.
- Static parameters can include things like quality of DR capabilities, Geographic spread, Compliance with industry specific standards, Ease of use, Security capabilities etc.

Appropriate scores can then be assigned to each CSP to measure them against the set of pre-defined QoS parameters.

Here issues associated with QoS in cloud setups are detailed , to provide insight to areas where best effort solutions may not be sufficient and hence pave way for innovation.

1. Performance

Virtualized infrastructure facilitates the property of on-demand use by encapsulating the operating and runtime environment for an application into a VM and being able to deploy it based on its resource requirement. However, current technologies tend to size VMs based on pre-defined static sizes and the user has to choose a close or near match for his/her requirements. This results in under-utilization of resources for the cloud provider and increased cost for the user. Also, lack of association between the variability of the hosted workload to the underlying resource provisioning mechanisms does not allow the user to exploit the cloud's elasticity property for his benefit. In addition, most resource providers' deal with resources in a disparate ways—CPU capacity along with fixed sizes of memory or storage blocks. What a user really needs is a composite set of resources, like the complete resource tuple, detailing properties of CPU, memory, network interface, and storage. It is essential that the QoS property holds for this composite set and not an individual resource. All resource managers need to make VM placement decisions based on such a composite resource to guarantee performance.

As one moves from the IaaS to PaaS and SaaS complexity in terms of quantification, measurement and assurance increases. It is essential to tie-up and build these features bottomup so that end-to-end performance guarantees can be achieved. This requires innovation that would lead to optimized usage of resources at lower costs to the user without compromising on his/her end user experience.

2. Availability

Compute clouds have evolved with a well-noted property to be used, that of resource availability, but how this availability can be specified and provisioned for is still nebulous. Here again the movement to cloud requires explicit specification. How does a provider allow the user to specify his availability requirements and how does he/she ensure that the requirements are met? What mechanisms does a cloud provider offer for assuring that the user's requirements are met? Many such questions need innovative solutions.

3. Security

Security is one of the key concerns perturbing cloud users. Independent and provider-specific mechanisms only elevate these concerns. One innovation that associates QoS properties to the functionality of security, addresses a means to ensure user's expectation on security. It is essential to understand security not just in its functional specification, but also how it enhances the user perception of the functionality. How to characterize and associate QoS attributes to security functions is a challenge. Security is closely associated with the architecture implementing a cloud solution. Normalizing security associated QoS from its implementation alleviates this dependency. How to do this is yet another challenge.

4. Jurisprudence

Clouds bring the globalization aspect into computing. In so far as the public clouds are concerned, providers would choose to setup their data centers in competitive geographical locations that can meet their infrastructural support requirements. However, unless legal frameworks dealing with specific issues of localization of data with regard to its geographical relevance are brought in, residence of sensitive data within its legal geographical boundaries may be mandated. Service providers need to address this issue, particularly in cases where e-Governance, health, surveillance, etc., associated applications are concerned. It is an interesting aspect and thus has scope for innovation, to explore how provisioning can be done keeping jurisprudence as the constraint.

5. Reliability

April and May of 2011 showed significant publicized outages, which raised a prominent question for public cloud reliability and availability:

- Amazon Web Services (AWS) was found inaccessible to data as well as service.
- Google's Blogger blogging service was unavailable to the bloggers, which resulted in inconvenience to the users.
- Microsoft's BPOS Exchange service also got hit by serious outage.
- Cloud Foundry, a new VMware public platform as a service (PaaS) offering for web developers, suffered sporadic downtime over two days due to a power outage and subsequent remedial activities.

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

Billing and metering re-verification is an important factor in building customer trust and thereby to increase adoption of cloud services. There are two common approaches for doing this:

- The first relies on cloud customers creating their own or using third party tools/mechanisms on their end to keep track of usage and compare the same with CSP provided information for each billing cycle. This is very similar to an individual mobile user using a third party app for measuring data usage on mobile phones and comparing it with the info provided by the mobile service provider at each billing cycle. While there are many apps that do this, they are not very accurate and one can't use that to dispute the mobile provider's measurements. A similar approach for cloud services will have similar issues and a third party measurement may not be acceptable to the CSPs. Moreover, this approach, not being very reliable, is not recommended except in very simple cloud scenarios.

- The second approach is based on the CSPs submitting their **monitoring and billing systems for audit by certified auditors** on a regular frequency and such certifications being made visible to the customers. TRAI can mandate the CSPs to get their billing and metering methods/tools audited by independent third party or a standards body similar to BIS. Once audited, cloud customers should have full confidence in the CSP's billing and metering mechanisms and will not require re-verification at each billing cycle. This approach is also preferred since it does not require each customer to have access to the CSP's internal systems and billing tools which are required for a trustable independent verification.

In addition to recommending the second approach based on audited and certified billing services, we also recommend that TRAI require CSPs to enable the following:

- **Online interfaces for real-time monitoring** the billing and metering of services
- Instantaneous/periodic feedback mechanism
- Storing of transaction logs at at-least coarse granularity.
- Billing dispute resolution mechanism (Nodal , Appellate and Ombudsman)
- Proactive, automated auditing at orchestrator level specifically directed for this purposes

CSP should adhere to standards for metering in cloud management

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

Our Response

Each CSP must be required to provision a customer issues management system that defines escalation paths in case of continuing issues.

Today most CSPs provide such systems via different levels of support (based on cost).

They also define the initial point of contact for issue resolution and an escalation matrix (internal or external) to resolve longer running or more complex issues.

TRAI should require CSPs to make their issue resolution mechanisms very transparent and open to the user community. However, final resolution and associated support costs etc should be left to the agreements between the cloud customer and the CSP.

In situations where the CSP is unable to resolve customer issues, an external agency or a central mechanism like an Ombudsman for Cloud services can be considered.

TRAI may also consider setting up sector-specific Cloud Management Office .

CMOs that can help resolve customer issues within the specific sectors or verticals.

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. **Information assurance** has been a long-standing practice since the traditional boxed product and on-premises systems era. Many governments today have established IT security programs that address risk-based processes (such as data classification schemes, lifecycle management, etc.), policies, and governance models. Many of these can be re-used and adapted for a cloud environment, whereas others (e.g. physical asset management) may need to be reapplied or deprecated. Because cloud moves much faster than traditional IT products, cloud assurance programs must be calibrated to match the pace of technology while still meeting the established security bar.

   Achieving that goal requires a rethink and active risk-based decision making at every step of a government's process of developing and implementing a cloud assurance program, as well as a clear understanding of the different roles and responsibilities involved. Having an effective governance model can clarify the roles and responsibilities for government and third party stakeholders alike – these are necessary to consider risk and efficiency and to determine whether new technologies are able to be consumed. In addition, determining data and system sensitivity and criticality requires a government to weigh the relative risks related to the confidentiality, integrity, and availability of different data sets and systems.

   There exist, very mature best practices, principles, and implementation guidance materials that would support governments as they develop and implement policies and programs to migrate their data and systems to cloud services. Among both the principles and implementation guidance, some common priorities are: Leverage global standards, enabling governments to achieve a high level of security with maximum agility and efficiency; and assess and manage unique risk scenarios not mitigated by global standards through a a risk-based approach. Governments that establish ongoing authorization processes that represent a subset of concerns and controls evaluated in the initial authorization process also ensure that highest priority risks are regularly evaluated.

   The core principles of trusted cloud are security of operation, data protection and privacy, compliance with local requirements and transparency. We encourage the government to consider these in developing a risk-based, agile cloud procurement environment. Ultimately, a risk-based approach must also be instilled through continuous improvement, a process during which governments evaluate how effectively risks are being managed and how risk priorities might be shifting.

2. 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. 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.

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 instill 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. We also need to understand the **importance & relevance of a multi-tenant environment**. Multi-tenancy or in other words resource pooling refers to a such an architecture in software environment where a single instance of software that runs on a server can work for different groups of people, while each is isolated from other.

   A tenant is essentially a group of people say for example any organization or company who share a common access with each having specific privileges to the software instance. With a multitenant architecture, a software application is designed to provide every tenant a dedicated share of the instance – including its data, configuration, user management, tenant individual functionality and non-functional properties.

   Many regard this Multi-tenancy architecture to be one of the major attributes of cloud computing. To make the above discussed architecture work, virtualization technologies are used. However, it's known fact that these underlying components that make up this cloud infrastructure are not designed to offer strong isolation amongst different tenants and there is always a risk of guest operating systems gaining huge amounts of access or control to the platform itself which makes it bit vulnerabilities.

5. 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.

   - Mandatory hosting of services or data processing and storage , within jurisprudence

     (within country), for all sensitive and confidential data / PII / Government data / as mandated by regulatory requirements.

   - Mandatory sharing Third party attestation / reports of industry standard compliances , audit test reports / Vulnerability & Threat Mitigation reports, for all equipment, be it of the CSP or the user, which is introduced in any cloud production environment.

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

- **Processes and Procedures.**
  1. It should be mandatory for the CSPs to share their security governance processes and capabilities.
  2. 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.
  3. Mandatory provisioning of information (Information Sharing) about any breach of security in any domain, viz physical, Network, systems and applications.
  4. Mandatory Compliance to a process driven Change Management before implementation of any change in the cloud environment.
  5. Mandated declaration, by the CSP, of the RA process for the technical support of the cloud infrastructure.
  6. Mandatory for the CSPs to ensure that their systems are updated with the latest OS patches and security software updates.
- **Certifications.**
  1. **Singapore's MTCS Certification Scheme[4].** 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 IS027018:2014, MTCS to ISO27001:2013 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.
  2. **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.**
- **User SLAs offered.**
  1. The CSP should be mandated to demonstrate its risk based management processes for control of information security.
  2. Mandatory provisioning of Root Cause Analysis of any failure , on it's closure.
  3. 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.
  4. Mandatory provisioning of activity logs for audit purposes.

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

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.

6. Promulgation of laws, Regulations and Other Mandates**.**

- 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.

- 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).

Beyond this security and compliance requirements for business should be understood by the customer and customer should select appropriate cloud service model ensuring it has necessary 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.

7. Suggestions on Building Security [REF8]

The following features and principles allow customers to align their security needs with cloud services, and are likely to become competitive differentiators over time:

• **Support APIs for security functions:** Cloud platforms and infrastructure shouldn't merely expose APIs for cloud features; but also for security functions such as identity management, access control, network security, and whatever else falls under customer control. This enables security management and integration. Don't require customers to log into your web portal to manage security. But do expose all those functions in your user interface.

• **Provide logs and activity feeds:** Extensive logging and auditing are vital for security — especially for monitoring the cloud management plane. Expose as much data as you can, as quickly as possible. **Transparency** is a powerful security enabler provided by centralization of services and data. Feeds should be easily consumable in standard formats such as JSON.

• **Simplify federated identity management:** Federation allows organizations to extend their existing identity and access management to the cloud while retaining control. Supporting federation for

dozens or hundreds of external providers is daunting, with entire products available to address that issue. Make it as easy as possible for your customers to use federation, and stick to popular standards that integrate with existing enterprise directories. Also support the full lifecycle of identity management, from creation and propagation to changing roles and retirement.

• **Extend security to endpoints:** We have focused on the cloud, but mobility is marching right alongside, and is just as disruptive. Endpoint access to services and data — including apps, APIs, and web interfaces — should support all security features equally across platforms. Clearly document security differences across platforms, such as the different data exposure risks on an iOS device versus an Android device versus a laptop.

- **Encrypt by default:** If you hold customer data, encrypt it in motion and at rest. Even if you don't think encryption adds much security, it empowers trust and supports compliance. Allow customers to control their own keys if they prefer. This is technically and operationally complex, but becomes a competitive differentiator, and can eliminate many data security concerns and facilitate cloud adoption.

- **Maintain security table stakes:** Different types of services, handling different types of workflows and data, tend to share a needed baseline of security. Fall below it and customers will be drawn to the competition. For example, IaaS providers must include basic network security at a per-server level. SaaS providers need to support different user roles for access management. These requirements change over time, so watch your competition and listen to customer requests.

- **Document security:** Provide extensive documentation for both your internal security controls and the security features customers can use. Have them externally audited and assessed. This allows customers to know where the security lines are drawn, where they need to implement their own security controls, and how. Pay particular attention to documenting the administrator controls that restrict your staff's ability to see customer data and audit when they do.

References:

[REF1] Liu et al. "NIST Cloud Computing Reference Architecture (Special Publication 500-292)", 2011

[REF2] Vince Lo Faso, "Understanding NIST's Cloud Computing Reference Architecture: Part II"

[REF3] CSA, SECURITY & RISK MANAGEMENT

https://research.cloudsecurityalliance.org/tci/index.php/explore/security_risk_management/

[REF4] Dan Sullivan, "Security as a Service: Guide to Cloud Solutions", 2014

http://www.tomsitpro.com/articles/security-as-a-service,2-691.html

[REF5] Richard Moulds, "SECaaS not just a security sideshow",

https://www.thales-esecurity.com/blogs/2013/november/secaas-not-just-a-security-sideshow

[REF6] CSA, SecaaS Implementation Guidance: Category 2: "Data Loss Prevention", 2012

[REF7] Securosis, "EXECUTIVE SUMMARY: The Future of Security", approved by the Cloud Security Alliance, 2014

[REF8] Securosis , "The Future of Security: The Trends and Technologies Transforming Security", Version 1.0, 2014

[REF9] Security Guidance For Critical Areas of Focus in Cloud Computing v3.0

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

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. 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. 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[5].

    b. 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.

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

    d. 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.

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

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

    g. 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.

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

h. 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.

i. 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.

j. 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.

k. 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.

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

m. 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.

n. 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.

o. 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.

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

Cloud security is shared responsibility - cloud environments result in shared security responsibilities between cloud service providers and customers

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. As ministries and agencies determine which data, systems, and services they want to migrate to the cloud and how they will manage risks, they should also consider which cloud service and deployment models are most fitting for their needs. In each of the cloud service models, the responsibility for various security functions is divided between the cloud service provider and the ministry or agency or customer. As a reminder, there are three major types of cloud services models: IaaS, PaaS, and SaaS.

   - * IaaS pools hardware resources for compute, storage, and connectivity capabilities, over which a customer can deploy and run operating systems and applications (i.e., PaaS and SaaS).

   - * PaaS delivers application execution services and often an operating system, enabling customers to create and deploy their own applications (i.e., SaaS) with greater agility.

   - * SaaS, also referred to as "on-demand software," delivers ready-to-use applications, such as e-mail, customer relations and management systems, or Microsoft Office, on scalable cloud infrastructure.

3. In any service model, the cloud service provider manages the underlying cloud infrastructure—the datacenters that power the cloud service. However, responsibility for various security controls otherwise varies. As a result, risk scenarios related to customer control requirements may respond

most noticeably to architecture decisions that alter these responsibilities and corresponding levels of control. Systems and data sets over which governments want to retain greater structural control, for instance, may be more suitable for IaaS or PaaS solutions, within which governments have more flexibility regarding security implementations. Alternatively, for SaaS solutions, cloud service providers take on a great degree of responsibility for the implementation of security controls, reducing the breadth of customer responsibility compared to IaaS or PaaS solutions.

4. In any service model, coordination between cloud service providers and ministry or agency customers is key. Therefore, in addition to assessing cloud service providers, governments should also carefully assess ministry or agency implementation of security controls; cloud environments result in shared security responsibilities between cloud service providers and customers. In each service model, government customers and cloud service providers may have full or shared responsibility for certain security controls. For instance, SaaS providers are responsible for managing service-level capabilities, which include employing security best practices such as penetration testing and defense-in-depth to protect against cyber threats. SaaS providers are also responsible for physical and data security in the form of employee access controls, encryption of data in transit, and enabling strong authentication. However, customer responsibilities include user identity and access controls, device management, and data management (e.g. rights management services, data loss protection), which are unique activities that the customer must implement. These security activities, which are under the customer's purview, empower the customer to control, access, and protect its own data.

5. **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.

6. **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.

7. **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 user’s responsibility to ensure proper cyber hygiene for the user’s devices and equipment.

Service Model	**Responsibility**
Software as a Service	● It provides the most integrated functionality built directly into the offering, with the least consumer extensibility, and relatively high level of integrated security. ● Security controls and their scope are negotiated into the contracts for service. Response activities will likely reside almost entirely with the CSP
Platform as a Service **And** **Infrastructure as a Service**	● In the case of PaaS or IaaS, it is usually the responsibility of the consumer's system administrator to effectively manage the residual services specified in SLA, with some offset expected by the provider for securing the underlying platform and infrastructure components to ensure basic service availability and security. ● In IaaS model, cloud consumer is responsible for securing and managing the operating systems, applications, and content. Example 1: Amamzon AWS EC2 IaaS includes vendor responsibility: physical security, environmental security, and virtualization security. The consumer is responsible for IT system: OS, Applications, and data. (related to security). Example 2: Salesforce provides entire security controls. Consumer is having operational responsibility.
Cloud Consumer	● Capability for detecting and responding to security incidents may reside with the customer. ● If there is no SLA, consumer will administer all aspects of cloud under its control.
Note : At the time of data transfer: collector/custodian of the data is responsible for securing the data	

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. 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.**

    c. E.g1. Under article 25 of the 1995 Data Protection Directive of 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. The recent activities of bulk surveillance by the US law agencies prompted a review of the 'Safe Harbor agreement' between EU and the US as the same was ruled to be not in compliance with the data protection laws in the US by the European Court of Justice. The renewed version of this agreement, known as the 'Privacy Shield', though has been criticized for not fully eliminating the concerns of bulk surveillance practices in the US, but it has laid down seven privacy principles, as given below, which are to be followed to enable any system of cross border transfer of data among various jurisdictions.

        i. Notice: Individuals must be informed that their data is being collected and how it will be used. The organization must provide information about how individuals can contact the organization with any inquiries or complaints.

        ii. Choice: Individuals must have the option to opt out of the collection and forward transfer of the data to third parties.

        iii. Accountability for Onward Transfer: Transfers of data to third parties may only occur to other organizations that follow adequate data protection principles.

        iv. Security: Reasonable efforts must be made to prevent loss of collected information.

v. Data Integrity & Purpose Limitation: Data must be relevant and reliable for the purpose it was collected.

vi. Access: Individuals must be able to access information held about them, and correct or delete it, if it is inaccurate.

vii. Recourse, Enforcement & Liability: There must be effective means of enforcing these rules.

2. E.g2. 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[6] of The Channel News Asia, "the US has such mutual assistance treaties with more than 50 countries, including Ireland".

3. **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").

4. 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

[6] http://www.channelnewsasia.com/news/business/microsoft-wins-appeal-to/2958542.html

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.

5. The lack of an overarching and comprehensive privacy and data protection law in India makes it difficult to evaluate adequacy of other countries wherein the data of Indian citizens would be transferred through these CSPs. In addition to the Privacy Shield principles enumerated above, for formulating a comprehensive framework to evaluate a complete and secure system of transmission of data from one jurisdiction to another, while balancing the privacy & choice of the user, it is suggested that any regulation for transferring of data between jurisdictions should include the following principles as well,

    a. Consumer protection & grievance redressal: An appropriate methodology for the user to lodge a complaint in their home country in their data is misused across borders in the foreign jurisdiction.

    b. Obligation to protect citizens' data from access by foreign intelligence services: There should be an explicit clause that excludes the transferred data from the purview of access by foreign intelligence agencies, or provisions such as bulk collection or processing by these agencies.

6. **Need for Cloud Computing Sectoral Laws.** Just as India has sectoral laws for the banking sector, Credit companies, Telecommunications, etc and Code of Ethics like those of the Doctors, Cloud computing being an emerging field should have its focused set of sectoral Laws and industry ethics that govern various aspects of B2B aand B2C business. It is suggested that the professional wisdom of bodies like the Cloud Computing Innovation Council of India (CCICI) can be tapped to evolve the Code of Ethics for this industry.

Our Recommendations

7. **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.**

    c. **Cloud computing being an emerging field should have its focused set of sectoral Laws and industry ethics that govern various aspects of B2B aand B2C business.**

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. Some countries have sought to exert greater control over citizens' data through strict data localization laws i.e. through legal provisions mandating the retention of citizens' data within national boundaries. Russia's new data localization law, Federal Law No. 242-FZ for instance, was adopted as a set of amendments to Russia's On Personal Data Law in July 2014 and came into force on September 1, 2015[7]. The law requires "operators" to collect, store, and process Russian citizens' personal data using databases located within Russia.7 Additionally, operators also must inform Russia's Roskomnadzor, the state body that oversees telecommunications, information technology, and mass communication, of the location of the servers where Russians' personal data is stored. Internet addresses that are found to be out of compliance with the law may be blocked[8]. While strict data localization laws such as these may appear to be potential workarounds that allow greater control over citizens' data and by extension, easier conduct of lawful interception by LEAs, this is far from true. While, the practical difficulties – both technical and financial – involved in restricting online activities to particular geographic boundaries may prove crippling for smaller Internet-based entities without vast resources at their disposal, however, for LEA requirements local hosting should be mandated, especially for services with a large user base in India.

3. 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

[7] Federal Law No. 242-FZ of July 21, 2014 on Amending Some Legislative Acts of the Russian Federation in as Much as It Concerns Updating the Procedure for Personal Data Processing in Information-Telecommunication Networks (with Amendments and Additions), available at: https://pd.rkn.gov.ru/authority/p146/p191/

[8] Courtney M Bowman, A Primer on Russia's New Data Localization Laws, August 27, 2015, available at: http://privacylaw.proskauer.com/2015/08/articles/international/a-primer-on-russias-new-data-localization-law/

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[9]. Some examples of multilateral MLATs are,

a. Convention on Mutual Administrative Assistance in Tax Matters.

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

4. 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%[10]. 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[11]) 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

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

6. **India should encourage local hosting of servers and applications, especially for services with a large user base in India.**

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. The various

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

[10] http://royal.pingdom.com/2010/07/27/top-20-countries-on-the-internet/

[11] http://www.channelnewsasia.com/news/business/microsoft-wins-appeal-to/2958542.html

models for deployment of cloud computing infrastructure, i.e. IaaS, PaaS and SaaS clearly reflect the same. 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. Refrainment from overly burdensome regulations as applicable to Internet-based services is also reflected in the National Telecom Policy 2012 (NTP). Moreover, cloud service providers are already regulated by a number of general and specific legislations that prescribe numerous general, technical, financial, and security related conditions that they must necessarily comply with. Some of the existing legislations that apply to cloud providers are:

    a. Information Technology Act, 2000.

    b. Consumer Protection Act, 1986.

    c. Payment and Settlement Systems Act, 2007.

    d. Indian Copyright Act, 1957.

    e. Income Tax Act, 1961.

    f. Customs Act, 1962.

    g. Central Excise Act, 1944.

    h. Foreign Exchange Management Act, 1999.

    i. Prevention of Money Laundering Act, 2002

3. **Singapore's MTCS Certification Scheme[12].** 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 IS027018:2014, MTCS to ISO27001:2013 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.

4. Similar to the Singaporean model of light touch regulation, in our opinion, the CSPs should be asked to register themselves as Other Service Providers (OSPs) with the government of India. As brought out earlier, given the global footprint of CSPs services, it is best to enact

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

and strengthen other laws and agreements for bringing the violations of CSPs into the scope of law.

Our Recommendations

5. **Cloud computing should not be subjected to the Indian Telegraph Act 1885 and should be dealt with a light touch regulatory regime.**
6. **CSPs should be asked to register themselves as Other Service Providers (OSPs) with the government of India.**

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

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

(b) promoting establishment of data 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.

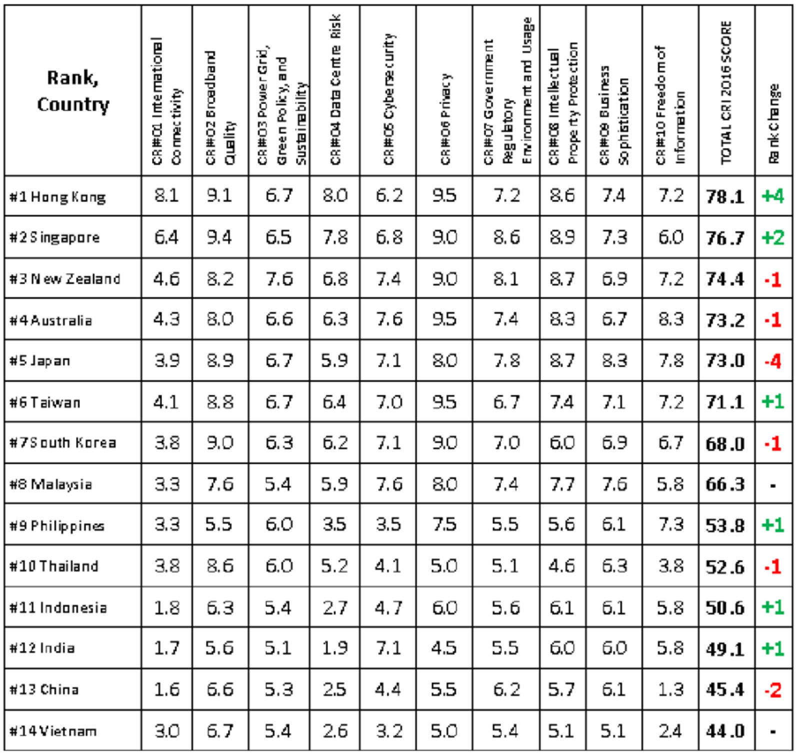
   a. **Subsidize power for development of domestic content hosting services.** Industrial Power rates vary from State to state. In an Internet Data Centre, Power is the most critical cost element which due to its high costs makes hosting of content unviable in India as compare to developed countries across 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 (i) Real Estate i.e space for developing a Data Center, (ii) Power for IT systems and environmental conditioning purposes and (iii) 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	CR#01 International Connectivity	CR#02 Broadband Quality	CR#03 Power Grid, Green Policy, and Sustainability	CR#04 Data Centre Risk	CR#05 Cybersecurity	CR#06 Privacy	CR#07 Government Regulatory Environment and Usage	CR#08 Intellectual Property Protection	CR#09 Business Sophistication	CR#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. There is need to have a holistic view of development and amongst the different approaches suggested based on different international cloud standards, the best one to deal with issue of interoperability in cloud is the Open Cloud Computing Interface (OCCI). It builds upon

World Wide Web fundamentals by using the Representational State Transfer (REST) approach[13] for interacting with services. 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[14]. OCCI is also compatible with existing standards such as the Open Virtualization Format (OVF) and the Cloud Data Management Interface (CDMI)[15].

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 cloud setup hosting only the governmental services.** Such a 'Government Cloud' can have the following characteristics:
   a. Use open standards based cloud computing technologies for enabling multiple interoperable cloud environments.
   b. Such cloud environments may be managed and used at different levels of governance e.g state government, rural and urban local government bodies etc.
   c. They can easily be deployed together or separately depending on their scale of operation and availability of resources and can be transitioned between such stages with little effort.

[13] http://www.ics.uci.edu/~fielding/pubs/dissertation/rest_arch_style.htm

[14] 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.

[15] https://www.infoq.com/articles/open-interoperable-cloud

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.