Broadband India Forum
BIF
...enhance, expand & unleash the true value of broadband

BIF RESPONSE TO TRAI CONSULTATION PAPER ON CLOUD COMPUTING

Introduction:

Role of Cloud Computing - Contributing towards the Digital India, Digital Economy

- "India aims 6% share in $300-bn global IoT industry in the next five years". M2M is going to change the role that communication and technology will play. There is a world of 50 billion connected devices envisioned by 2020. The cloud computing along with the mobility and ubiquitous broadband will be playing a crucial role for a connected economy vision of the Government of India.

- Cloud computing is attractive to consumers and the businesses because of its efficiencies, convenience and affordability. The Global cloud computing services market is expected to reach US $127 billion by 2017

- A policy regime that allows full benefits of cloud computing to be leveraged with the goal of affordable internet services to all should be the key. A regulatory framework which encourages competitive market should be encouraged.

Offering Cost Benefit – Economies of scale and cost reduction

Cloud computing reduces the infrastructure cost significantly with the data centre cost also going down due to economies of scale. Since cloud networks operate at higher efficiencies and with greater utilization, significant cost reductions are often encountered.

Reduced Upfront Costs: Most technology projects have a ramp up period that could last one to six months, when usage is low. Reducing spending of CapEx (capital expense) on equipment and software and moving that investment to the cloud (OpEx – operating expense) allow companies to better align investment and cost with actual usage, lowering the total cost of ownership.

Usage-based Pricing: A lot of effort and resources are required in acquiring the equipment, deploying the equipment in a data center and then configuring the environment for the end user (engineering, R&D, marketing, application developers). End-users of cloud computing pay only for the resources they use. For example, a cloud end-user may need to use ten servers to test and develop an application over the course of a few months. Rather than having to buy the hardware, colocation space and power to support the temporary project, you can simply use ten cloud-based servers for two months.

Automated Infrastructure Management: The efficiency of cloud computing reduces the amount of time which IT systems administrator on managing and supporting infrastructure. The

average number of server administrators to servers in a typical data center is 50 servers: 1 administrator. The average ratio of cloud-based data centers is 500:1.

Outsourced IT management: A cloud computing deployment lets someone else manage your computing infrastructure while you manage your business. In most instances, you achieve considerable reductions in IT staffing costs.

Operational Services and Support: By leveraging the managed services of a cloud provider and systems integrator, companies can reduce the cost of managing and maintaining their web server, database and middleware software and systems; collaboration; mobility; storage; backup; and enterprise applications.

Reduced Downtime: being able to spin up a temporary environment of servers, storage and networking allows IT to more quickly troubleshoot issues that lead to system downtime. Adjusting the processing power, memory and storage performance of a server during troubleshooting can quickly eliminate the possibility of system utilisation being a constraint.

Virtualization: using virtualization technology creates multiple virtual machines on a single physical machine can significantly reduce the hardware and power costs. Most large enterprises have already implemented virtualization.

Resource leverage: multi-tenant architectures (in a private our public cloud) allow users to take advantage of better leverage and economies of scale for IT resources.

All the above factors towards cost reduction make Cloud Computing an apt environment for SME. Overall reduction of computing costs can also greatly reduce barriers to market entry for SMEs, allowing for greater levels of innovation and growth. Cloud computing allows SMEs to scale more effectively because they can buy computing services as needed instead of making large upfront investments in data center infrastructure.

Other Benefits/ Features for Cloud Service:

The cloud computing solution offers countries to meet the Energy efficiency target and other Global and domestic issues like security, public safety and affordability.

1. **On-demand self-service:** A client can provision computer resources without the need for interaction with cloud service provider personnel.

2. **Broad network access:** Access to resources in the cloud is available over the network using standard methods in a manner that provides platform-independent access to

clients of all types. This includes a mixture of heterogeneous operating systems, and thick and thin platforms such as laptops, mobile phones, and PDA.

3. **Resource pooling:** A cloud service provider creates resources that are pooled together in a system that supports multi-tenant usage. Physical and virtual systems are dynamically allocated or reallocated as needed. Intrinsic in this concept of pooling is the idea of abstraction that hides the location of resources such as virtual machines, processing, memory, storage, and network bandwidth and connectivity.

4. **Rapid elasticity:** Resources can be rapidly and elastically provisioned. The system can add resources by either scaling up systems (more powerful computers) or scaling out systems (more computers of the same kind), and scaling may be automatic or manual. From the standpoint of the client, cloud computing resources should look limitless and can be purchased at any time and in any quantity.

5. **Measured service:** The use of cloud system resources is measured, audited, and reported to the customer based on a metered system. A client can be charged based on a known metric such as amount of storage used, number of transactions, network I/O (Input/Output) or bandwidth, amount of processing power used, and so forth. A client is charged based on the level of services provided.

Regulatory Framework

While deciding the **regulatory framework** the core principles of cloud computing should be taken into account. The objective should be to enhance the growth of internet and access to Internet in a secure and safe manner, ensuring cost effectiveness, which is the key to cloud computing.

Principles for Cloud Computing

- The framework should **encourage innovation**
- **Enable flexibility to allow choice of cloud architecture**
- **Data security, Protection and Data awareness:** The Government should seek to align data protection regimes with internationally accepted models so that it will ensure continued global data flows with other countries or regions.

  Regardless of whether cloud computing is to be the subject of specific statutory regulations in the future, the data protection provisions that apply to cloud computing, the three issues are of importance:

  - the conditions under which the transfer of personal data processing to third parties is permissible;
  - the conditions under which personal data may be sent abroad; and

- the privacy & security data itself.

- **Privacy & Transparency:** One size fits all' approach to the cloud cannot work. For instance, the public cloud is effective for an organization handling high-transaction/low-security or low data value (e.g., sales force automation). Private cloud model, on the other hand, may be appropriate for enterprises that face significant risk from information exposure such as financial institutions and health care provider or federal agency. For medical-practice companies dealing with sensitive patient data, which are required to comply with the HIPAA rules, private cloud may be appropriate. Today, accurately or not, businesses are concerned about issues such as privacy, availability, data loss (e.g., shutting down of online storage sites), data mobility and ownership (e.g., availability of data in usable form if the user discontinues the services). Many of the user concerns can be addressed by becoming more transparent.

  While we understand that India seeks to provide greater assurance that Cloud computing services provide adequate security, levels of service and data privacy protections, many of these issues are already addressed in different government policies or by vendor practices (such as contracts).

- **Adherence to standards:** When one considers the development of cloud computing to date, it is clear that the technology is the result of the convergence of many different standards. Cloud computing's promise of scalability completely changes the manner in which services and applications are deployed. Without standards, the industry creates proprietary systems with vendor lock-in, sometimes referred to as "stovepipe" clouds. Because clients do not want to be locked into any single system, there is a strong industry push to create standards-based clouds.

  The cloud computing industry is working with these architectural standards:

  - Platform virtualization of resources has the capability to ensure that the user get dedicated and secured resources on the shared platform. The technology behind virtualization has improved markedly over the past few years benefitting the cloud computing offering.
  - Service-oriented architecture
  - Web-application frameworks
  - Deployment of open-source software
  - Standardized Web services
  - Autonomic systems
  - Grid computing

- **Broadband and connectivity** offers more opportunity for the cloud resources to be leveraged. With more wireless options customers can also manage and access their

resources from mobile devices. Improved connectivity is an important factor that not only the enterprise but individual consumers are migrating their resources to public and private network.

- **Principles of Reliability, Scalability Interoperability:** The scale of cloud computing networks and their ability to provide load balancing and failover makes them highly reliable, often much more reliable than what you can achieve in a single organization. Features which can support reliability & scalability of the cloud should be promoted.
- **Offer Competitiveness:** The policy regime should allow competitiveness which is inherent in the DNA of Cloud computing due to its capability to provide dynamic, elastic resource pool with flexible environment, reducing financing and integration requirements.

By offering location independence and ease of collaboration and access to all employees, Cloud computing can level the playing field between small medium and large organizations. Smaller companies can quickly enhance capacity & resources through Cloud computing while offering opportunity for technology advancement.

Virtualized resources in the cloud lower upfront investment and product development costs. However, the low cost comes with a trade-off. It is too simplistic to view the cloud as a low-cost security. Legitimate as well as illegitimate organizations and entities are gaining access to data on the cloud through illegal, extralegal, and quasi-legal means. The cloud's diffusion and that of social media have superimposed onto organizations' rapid digitization in a complex manner that allows cyber-criminals and cyber-espionage networks to exploit the cloud's weaknesses. Ensuring that both technological and behavioral/perceptual factors are given equal consideration in the design and implementation of a cloud network is thus crucial.

Quality of Service:

The Quality of Service (QoS) should be obtained under contract from the vendor offering Cloud Computing solution. Where appropriate, contractual requirements cloud be used by the customer to ensure the continuity of operations. However, mandated prescribed standards for cloud providers to handle data, processes and virtual machines developed on other platforms may hurt innovation, hence a balance is important to maintain.

Steps by Government in promoting cloud computing

The policy requirements for India should begin with developing a comprehensive and systemic framework for data centers. The motivation should be to create an enabling environment for private players to enter the market and to meet the growing needs of data management in India. Most importantly, it should be kept in mind that the data centre market is capital and technology-intensive.

While it may be believed that a data localization requirement may be an attractive means of forcing firms to build data centers in India, the quantitative and qualitative evidence in markets across the world indicate that such requirements serve as a disincentive for foreign firms to invest domestically and make it more expensive for local firms to enter and compete in the domestic market or compete and enter global or regional markets.

One of the trade barriers recognized by various studies done on promoting 'Digital Trade' & IOT include localization requirements for cloud computing as a major trade barrier. That means that instead of harnessing the economies of scale that come from a cloud, companies will be forced to house in facilities in individual countries, resulting in duplicative infrastructure and higher costs. Let us bear in mind that a location anywhere on the face of the earth is a location everywhere on the face of the earth. And it's not just technology companies that can be harmed by these types of digital trade barriers. In the financial services industry, banks use a security practice known as charting, that splits a single customer's information into discreet packets that are stored in multiple locations to prevent a hacker from compromising it. By its very definition, this practice would be impossible without the free flow of data.

Broadband India Forum (BIF) welcomes this opportunity to offer its comments on the TRAI Consultation Paper on cloud computing. This consultation comes at a critical time when India is at an inflection point in technology adoption with significant gains observed in mobile, and internet penetration. A key driver of India's rapidly expanding digital economy has been the emergence of cloud computing as a means to improve efficiency and scale, while minimising costs.

I. The Potential of the Cloud Revolution

Cloud technology has revolutionised the business and end-user landscape with innovative solutions being offered in communications, collaboration, and infrastructure provisioning. Today, cloud solutions form the backbone of many critical applications such as e-mail, telephony, instant messaging, productivity tools, as well as enterprise functions such as virtualisation, and conferencing. The Indian government with its pioneering Megh Raj national cloud service has also identified cloud technology as a key catalyst for improvements in service delivery, and e-governance.

With the uses of cloud technology rapidly increasing, the market is primed for a cloud computing explosion with accompanying gains to innovation, savings, and efficiency. Driven by high growth in segments such as Infrastructure-as-a-Service (IaaS), Software-as-a-service (SaaS), cloud management and security services, public cloud service revenues in India were estimated to have reached USD 731 million in 2015. These growth rates are expected to continue through 2019 when the Indian market is expected to reach USD 1.9 billion.[1] This is a reflection of the

[1] Gartner, "Gartner Says Indian Public Cloud Services Market Will Reach $731 Million in 2015" (Oct 26, 2015), available at http://www.gartner.com/newsroom/id/3156617

global trend which has seen revenues from IaaS grow more than 38% as increasing levels of IT application and services migrate to the cloud.[2]

However, cloud adoption in India is not without its obstacles. The most significant of these is the lack of high-quality internet infrastructure, power supply, national security concerns, and outdated policy frameworks ill-suited to the rapidly-emerging cloud paradigm. This has resulted in an uncertain and risk-prone operating environment for cloud service providers. The 2013 Data Centre Risk Index ranked India in a lowly 29th place of 30 countries in terms of several macro level risk factors – physical, economic and social, that could cause a threat to service continuity and uptime.[3] India was also ranked second-last (12th out of 14 countries) in a 2016 study which also ranked India last on parameters including power-grid, data centre risk, and business sophistication; and second from last on international connectivity and broadband connectivity.[4]

II. Policy-making for the cloud facilitation

Without policies and frameworks which ease, and facilitate, the adoption of cloud computing, the Indian digital economy would suffer competitively and lose out to other emerging economies. This would lead to the country missing a major opportunity to take advantage of the cloud revolution and the benefits it can bring for convenience, cost savings, productivity and governance. Therefore, there is an urgent need for the Indian government to re-examine its approach to policy-making for the cloud sector, and ensure the creation of a pro-ICT business environment capable of supporting migration to the cloud.

TRAI should take this opportunity to send a strong message to the world that India is ready to take advantage of the cloud revolution by evolving a framework premised on facilitating cloud adoption/migration and ease of doing business. In addition to improving physical cloud infrastructure including power and connectivity, India must create a policy environment facilitating trans-border data flows, harmonisation with international regulatory standards and best practices, and data centre facilitation.

At the same time, the government should refrain from imposing burdensome regulations which interfere with the free flow of data, stifle cloud adoption by creating an ambiguous or uncertain regulatory environment, and thereby harm overall national productivity. Policies such as forced/mandatory data localisation would strongly harm India's reputation as a global technology hub and affect savings, scalability and competitiveness of the country.

---

[2] Gartner, "Gartner Says Worldwide Public Cloud Services Market Is Forecast to Reach $204 Billion in 2016" (Jan 25, 2016), available at http://www.gartner.com/newsroom/id/3188817

[3] Cushman and Wakefield et al., Data Centre Risk Index 2013" (2013), available at http://www.cushwakedatacentres.com/downloads/data-centre-risk-index-2013.pdf

[4] Asia Cloud Computing Association, "Cloud Readiness Index 2016" (2016), available at http://www.asiacloudcomputing.org/images/documents/cri2016_acca.pdf

Following the government's guiding regulatory principle of 'Minimum Government, Maximum Governance', a system of minimal regulatory intervention for emerging technologies, products and business models is optimal to harness the economic and social benefits of the digital economy. In this regard, the government must undertake minimum regulation and instead may encourages frameworks such as voluntary compliance check-lists, encouraging self-regulation on issues such as security and interoperability. At the same time, core business decisions such as location of data storage must be left to respective service providers to decide. We firmly believe that these should be the guiding principles for government when attempting to regulate an emerging issue such as cloud computing.

With the above backdrop, BIF seeks to respond to the questions raised in the Consultation Paper

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.

BIF Response:

Cloud services are inherently global in nature, and India's policies should aim at creating Indian CSPs which are globally competitive rather than seeking to provide them a protected market. Such globally competitive providers would be of help to a whole range of Indian Industry, particularly SMEs.

a) (i) Base cost estimation: Since cloud computing uses on-demand pricing, it is important to calculate the cost of maintaining IT infrastructure in house. Though many authors suggest more sophisticated cost calculation model for cloud computing, on-demand pricing would still have its ubiquitous presence in all cost calculation methods.

(ii)Use of VM technologies:

The increasing availability of VM technologies has enabled the creation of customised environments on top of physical infrastructures. The use of VMs in distributed systems brings several benefits such as:

- Server consolidation, allowing workloads of several under-utilized servers to be placed in fewer machines;
- The ability to create VMs to run legacy code without interfering in other applications' APIs;

- Improved security through the creation of sandboxes for running applications with questionable reliability;
- Dynamic provision of VMs to services, allowing resources to be allocated to applications on the fly; and
- Performance isolation, thus allowing a provider to offer some levels of guarantees and better quality of service to customers' applications.

Existing systems based on virtual machines can manage a cluster of computers by enabling users to create virtual workspaces or virtual clusters.

(b)

It is believed that the cloud computing should provide consumers data storage and computing services in a secure, fast and the most convenient possible way. Cloud computing and ecommerce highly benefit from the Internet. Cloud computing allows consumers and clients to use services, computational resources and storage in a transparent way. E-commerce on the other hand, allows consumers to buy services or products from just about anywhere in the globe and anytime. The cloud computing for e-commerce has several benefits. The cost can be calculated based on the need of each company. According to Amazon, cloud computing helps businesses to significantly reduce the costs on several places such as hardware procurement, security, privacy, energy, and maintenance.

One of the most essential benefits of cloud computing is its ability to scale based on the demand of the cloud clients or businesses. Many of the operations such as activation of the server, increasing the computation power, to reallocating the loads due to changing demands on the cloud can take place relatively quickly (in the order of minutes). These operations basically define the scalability of the cloud and the flexibility to allocate more resources when requested and disposing of them when they are no longer needed by the cloud users.

In order to sustain the quality of e-commerce, the computing services must be scalable, reliable and provide flexibility of access to products and services from anywhere and anytime in the world. Many of the large cloud service providers such as Google, Amazon, IBM, and Microsoft have their data centers spread across the globe in order to guarantee reliability in accessing the cloud applications in cases of failures.

(c)

i. Employ a pay-for-use cost model. With that method, it makes sense to schedule regular server jobs and configure a baseline, then scale from that accordingly to meet demand.

ii. Schedule your servers to do backups every day.

iii. It can be a lot cheaper to store your archives in a cloud data center.

iv. Plan for failure in the cloud.

(d) NIL

Cloud Computing is one of the new paradigms and technologies to emerge out of the next generation school of technologies which along with social media, big data and smartphones is set to transform the way we live, the way we work and the way we communicate besides making relevant information and data accessible , affordable and available at any time, place , and anywhere .

Cloud Services viz. Cloud Computing are inherently global in nature and India should create an enabling policy and regulatory environment with the intent of creating Globally competitive Cloud Service Providers (CSPs) instead of seeking to provide restrictions by way of a protected market . This would involve doing away and avoiding unnecessary regulatory strictures and creation of an environment which shall foster promotion of innovation and entrepreneurship. Such globally competitive Service Providers in the cloud who adhere to internationally recognised and adopted standards would help the entire industry including SMEs.

Effective use of People, Process, Technologies & Partners enables Cloud Service providers to accelerate introduction of new services, thereby providing businesses the cutting edge.

a) For accelerating the design and rollout of services, the following may be considered:

-Enable improved IT efficiency and economies to reduce IT costs

-Shift from a Fixed Cost to a Variable Cost regime

-Migrate to Pay per Use to enable faster delivery of services

-Improve the agility and speed of government services

-Scalability to meet demand peaks

b) Cloud technologies helps in deployment of various collaboration tools and enables easy and speedy availability to its users. Start-up and e-commerce companies can leverage cloud technologies and quickly develop and deploy the applications . Cloud Technologies enables them to scale their infrastructure up and down as per requirement.

c) For rolling out of new services, deployment of Platform as a Service (PaaS) cloud model could be useful for quick deployment of new services , thereby enhancing business agility. This model augmented with Infrastructure as a Service Cloud model (IaaS) can provide both development and deployment environment which would be conducive for expediting development of new applications.

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?

BIF Response:

Cloud computing is a business model of delivering IT resources(Computing Power, IT infrastructure), applications, platforms & business processes as services accessible remotely over the Internet as general utilities to users in an on-demand fashion rather than locally. In the traditional model, IT resources and applications are provided in the form of products which are sold or licensed from a vendor to a user and then utilised locally on a local server based infrastructure. This new computing model has been made possible due to the rapid evolution of processing power, storage technologies & availability of High quality broadband speed & availability of Big Data. Cloud can provide scalability by automatic resource optimization as per the demand of the user and hence provide expansion of services on the go.

The benefits of Cloud Computing should not be only to reduce Capex but should be utilised to make the Indian businesses more competitive in the global markets. As regards the theory that due to economies of scale , use of Cloud Computing is bringing about cost reduction may be dependent on whether the workload or applications are growing at the same rate as the business itself or not. In the former case, to keep the data on in-premise Date Centers may prove to be more cost effective, especially if the latest infrastructure models are being used.

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?

BIF Response:
Cloud computing allows computer e-governance users to conveniently rent access to fully featured applications. .Cloud computing also provides software development and deployment environments, and computing infrastructure assets such as network -accessible data storage and processing model.
Enterprise of any size have manages risk associated with the use of IT. Vendors should be chosen appropriately like those are more capable of handling all the front-end and back-end processes of cloud services. Enterprise big or small needs to understand who is responsible for managing what risks, as well as where an external vendor is responsible and how capable it is of doing so effectively.

In case of large business enterprises, the main focus would be on the performance and security of their database. Large organizations usually prefer in-house capabilities to cater their needs. However in case of Small and Medium size Enterprises, the prime area of the focus would be cost saving, which can be best met through the cloud services as it involves lesser cost and easy accessibility as compared to conventional non-cloud services.

Cloud Services offer SMEs in particular the ability to not only manage costs but also security and even regulatory compliance more effectively.

Managing Risk is another major attribute which influences the decision to select the cloud models. All enterprises need to understand who is responsible for managing what risks are prevalent, where an external vendor is responsible and how capable it is of doing it effectively . Security often requires an understanding of the limits/edges of the compliance boundaries and as to which risks are the sole responsibility of the cloud vendor and which happen to be that of the customer himself.

Businesses categories applications/services based on various parameters viz. business criticality, performance requirement, security requirement, compliance, agility to deploy services, etc. Accordingly, such categories are then mapped to various cloud deployment models.

Business critical applications wherein key business sensitive data requiring access to large databases and high performance requirement prefer to opt for a Private cloud. Applications requiring flexibility, agility and which do not carry critical business data like development/operations are typically deployed on a Public Cloud. Applications requiring specialised Hardware and Software not normally used in regular IT operations are hosted on Public/Community Cloud. Of course, this is subject to these applications/services being outsourced and long term backup and archival data being suitable for public cloud. Hybrid cloud employing a mix of both is also becoming quite popular amongst most businesses.

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

BIF Response:
Application migration is primarily about moving them back and forth between private clouds and public clouds or from a public cloud to another public cloud. Application migration among clouds allows users to select best of breed cloud technology and avoid lock-in, but it's not possible without tools that facilitate communication between different cloud vendors and services.

- One of the first considerations is an organization's existing data center investment. Despite technologies such as server virtualization, there are real costs associated with deploying on-premises servers. There are not only licensing costs involved, but also costs associated with hardware resource consumption and support infrastructure. As such, there is almost always a significant investment associated with an **on-premises server**. Outsourcing a server's data and/or functionality to the cloud may mean abandoning your on-premises investment unless an on-premises server can be repurposed.
- In the case of application servers, administrators must consider whether the application can function in the cloud. Likewise, the application's performance must be considered.

- Compatibility usually isn't a big problem for newer applications that run on top of modern operating systems. It is also easy to assume that performance won't be an issue for such applications because most cloud providers will allow hardware resources to be allocated to hosted servers on an as-needed basis. It does little good to have a high-performance hosted application server if Internet bandwidth limitations stand in the way of a good user experience.
- Although it is often easy to migrate a virtualized application server to the cloud, the application might have external dependencies that rule out (or greatly complicate) a cloud migration. For example, the application might have an Active Directory dependency or require access to an on-premises SQL server database.
- For older applications that run on legacy operating systems, a move to the cloud may not be an option. Lab testing is the only way to know how an application will behave in a cloud environment. Testing helps determine the steps that are involved in moving the app there.
- Another consideration for moving application servers to the cloud is hardware scalability. Some IT analysts have suggested that cloud services are ideal for hosting hardware-intensive workloads because cloud services generally offer nearly unlimited scalability. While a cloud service provider can usually scale its offerings to meet even the most demanding workloads, this scalability comes at a price.

  BIF is of the opinion that a hard nosed prescriptive form of regulation may not be conducive to the growth of cloud computing and improving the working economic efficiency of the enterprise sector. It believes that the Cloud Service Providers should be allowed the flexibility to offer different approaches for migration of their customers and the same should be dictated by market forces and user choices instead of regulation. It is of the opinion that mandated prescribed standards for cloud providers to handle data, processes and virtual machines developed on other platforms will hurt innovation. Decision to retain data inside on-premises IT infrastructure and when and what to move to the cloud can be often a very difficult decision . The impact of such a decision on business transactions requires efficient and transparent multi-cloud mobility so that data can move across cloud providers as well as between on -premise IT infrastructure and the Cloud. Businesses need multi-cloud data and application mobility for their hybrid cloud environments for several reasons viz.

  - -reduce corporate risks
  - -accelerate time to market
  - -turn data into revenue
  - -lower cost of IT Infra
  - However, a prescriptive regulatory based approach for data movement is not recommended and is best left to innovative solutions from the Cloud Service Providers (CSPs) which should be based around the SLAs between the CSPs and their customers.
  - The Migration & Deployment should be in Phases. The Cloud Service Providers (CSPs) should use analytics to qualify the data and identify the best suitable ' data ' which are ready for transformation and migration to the cloud . For those applications that are fit

to be migrated to the cloud , an appropriate migration strategy is worked out keeping all parameters including financial viability in perspective. Using a mix of analytics, tools and automation, the cloud environment and the migrated data is subjected to virtualisation, standardisation, registration, testing and on-boarding is done.

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?

BIF Response:
Establish sets of criteria that help customers analyze and evaluate migration and exit concerns before adopting and deploying cloud computing solutions. Customer needs to have a regular back-up of its data by the cloud service provider .Users of cloud services should be in a position to evaluate those services, and their potential for lock-in, and also to set out in advance an effective exit and migration strategy. While recognizing that there is no "one size fits all", users of cloud services should have in hand lists of questions against which to consider any available cloud services in order to make sure that they are able to migrate information and functionality in view of the ever-changing business climate. Some example questions that can be built upon include:

- **With respect to IaaS cloud services:**
  Are the virtual machine packaging formats based on open standards? Are any lock-in concerns mitigated by source code access or use of open source components? Is it possible for existing workloads to be migrated between cloud services?

- **With respect to PaaS cloud services:**
  Does a PaaS service allow you to write applications and move them to another platform, including back to a more traditional platform? Do the applications running on the PaaS system rely on open packaging, deployment and run-time management interfaces? Are any lock-in concerns mitigated by source code access or use of open source components?

- **With respect to SaaS cloud services:**
  What format(s) can customer data be provided in? Are the formats based on open standards? Can cloud service customer data be retrieved from the cloud service in a standard format through an open interface?

- **For all cloud services:**
  Are common security requirements addressed through standard or open interfaces –for example, Identity and Access Management?

Additionally, the Indian government should seek to align data protection regimes with internationally accepted models so that it will ensure continued global data flows with other countries or regions such as the EU.
Data protection and privacy laws and regulations are designed to protect personal data. Government mandated regulations are likely to inhibit growth and innovation in cloud computing services and should be avoided. Instead, model contractual terms based on best international practices, maybe offered to the CSPs.

There are internationally accepted data protection regimes and models. Govt should seek to align to those , to ensure continued global data flow with other countries . In fact, BIF advocates that Govt should promote policies that advance the objectives of transparency to enable users of cloud-based services to make carefully considered and smarter decisions regarding the risk of lock-in.

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?

BIF Response:

Service provider interoperability is a critical component of ensuring that customer welfare and interests are protected. As public and private organizations shift to cloud computing, users should not overlook the implications of switching vendors in the future. Therefore, the government should encourage the formulation and standardization of open interfaces and data formats guided by open standards help to ensure users retain the ability to efficiently transfer their data in the future.

At the same time, the deployment of closed services which do not retain interoperability may be discouraged. However, the same is a business decision that should be left to the discretion of each entity. The government may provide further incentives to service providers who adhere to open standards but should not use the mandate of interoperability to force features on service providers. This would restrict the proliferation of diverse business models, and harm India's competitiveness on the global stage. As discussed above, a non-interventionist framework premised on a pro-innovation, pro-ICT approach should be privileged.

For interoperability, there are many challenges associated with cloud computing. In general, the interfaces and APIs of cloud services are not standardized and different providers use different APIs for what are otherwise comparable cloud services.

There are some practical approaches to handling these interoperability challenges. One possibility is for the cloud service customer to provide an isolation or mapping layer between

their own applications and systems and the cloud service interfaces, so that the cloud services are not invoked directly by customer applications.

Interoperability aspects of a cloud service mainly relate to the three interfaces between the customer and the cloud service – how users and applications in the customer environment interact with the functional, admin and business interfaces offered by the cloud service. It is important to understand that the interoperability of the three interfaces may be independent of each other and that the interoperability of one interface does not guarantee the interoperability of the others.

Standards and inter-operability are the key to the growth of the ICT industry which includes cloud computing. Standards setting should be driven using the internationally recognised standards development organisations (SDOs) with the aim of setting and/or working under an existing global framework. A variety of SDOs may be involved in standards setting in different aspects of Cloud Computing. Role of Government should be to encourage development and adoption of Open Standards related to Cloud Computing and to foster inter-operability through open and transparent processes. As a major purchaser of technology and implementer of standards, the Govt. should participate in standards setting activities and rely on consensus based standards.

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.

BIF Response:

Several challenges are tackled in realizing the model for evaluating QoS and ranking Cloud providers. The first is how to measure various SMI attributes. Many of these attributes vary over time. The second challenge is how to rank the Cloud services based on these SMI attributes. There are two types of QoS requirements which a user can have: functional and non-functional. Some of them cannot be measured easily given the nature of the Clouds. Attributes like security and user experience are not even easy to quantify. Moreover, deciding which service matches best with all functional and nonfunctional requirements is a decision problem. It is necessary to think critically before selection as it involves multiple criteria and an interdependent relationship between them.

QoS parameter should have suggested three setting in terms of performance: Minimum, Maximum and Burst Performance. This performance for example at a storage tier can be

measured in IOPS and MBps. These parameters should be measurable and demonstrable through the appropriate management software for respective element.

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?

BIF Response:
Cloud is a pure utility renting computing model where resources can be utilised as per client's need. In such a scenario , accounting of resources used and billed needs to be substantiated by the Cloud Service provider by preserving complete logs and all such other details which are essential for complete satisfaction of the client. This may be achieved by making provisions for the following:

-Timely receipt of Bill
-Accuracy & completeness of the Bill
-Clarity on the Bills'
-Presentation of Billing information in terms of transparency & clarity
-Transparent process of resolution of billing complaints

The Cloud service provider is required to be able to provide a SLA measuring tool to the client so that parameters agreed between the client & the service provider can be monitored by the client using SLA tool. Billing will obviously depend on performance or extent to which SLAs are met.

The CSP should provide an automated process (by measuring own use of the cloud) to verify that the actual bill matches the IT generated one. This should include measuring metrics that can result in penalties . However, in case of any discrepancy , as a part of the governance process, the client should submit the billing details to the CSP who in turn should validate the bill by providing the services provisioned and duration availed of , to resolve the discrepancy.

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

BIF Response:
Customers must consider the policy and compliance requirements relevant to them when reviewing a CSA since there are interdependencies between the policies expressed in the CSA and the business strategy and policies developed across the lines of business. The data policies of the cloud provider, as expressed in the CSA, are perhaps the most critical business level policies and should be carefully evaluated. The obligations a cloud provider has to its customers and their data is governed by a potentially complex combination of:
• customer requirements,

• the data protection legislation applicable to the customer as well as to its individual users (which may not be under the same jurisdiction in a multinational company)
• the laws and regulations applicable where the data resides or is made available.

Customers should carefully consider these legal requirements and how the CSA deals with issues such as movement of data when redundancy across multiple sites means subjecting the data to different jurisdictions at different times. The issue of jurisdiction takes on additional complexity when global compliance is taken into consideration and more than one cloud provider is used. In these instances the customer may have to coordinate negotiations between providers to ensure the necessary data management.

Critical data policies that need to be considered and included:

Data Preservation and Redundancy - Timely and efficient capturing and preservation of data is critical to maintaining the organizational memory of a business or the general user. Customers should therefore ensure they have an appropriate data preservation strategy that addresses redundancy within the system.

• Cloud customers should ensure the CSA supports their data preservation strategy that includes sources, scheduling, backup, restore, integrity checks, etc.
They should be concerned as to the protections offered or omitted by the service provider.
•It must be possible to test the CSA to demonstrate the required level of service availability.

Data Location - CSAs that cover locations under different jurisdictions are challenging. Customers should consider how the CSA specifies where their data resides, where it is processed, and how this meets the various applicable regulations. Customers should also understand where the data is viewed or delivered, and whether this results in a transborder data flow with regulatory or tax implications.

Data Seizure – Legal powers enable law enforcement and other government agencies to seize data under certain circumstances. Customers should ensure the CSA provides for sufficient notification of such events.

Customers should also ensure there are arrangements in place to make their data available in the event that their provider goes out of business.

Data Privacy - The provider's data privacy policy should be included in the CSA, and should ensure that the provider will conduct business in compliance with applicable laws on data privacy protection.

Data privacy in a cloud context is not just about the protection of the information about the customer's agents in its dealing with the provider (this is the narrow meaning in many existing

Service Level Agreements), it also includes the privacy of the information that may be stored about the customer's own customers.

Data Availability - Assess whether the provider's maintenance schedules might interfere with business processes subject to external constraints, such as financial reporting or the business's hours of operation in certain regions.

Change Management and Notification - The change management and change notification obligations of the provider should be carefully reviewed, especially the amount of time allowed to prepare for a change. The provider may also ask the customer to provide certain change notifications, which is a good opportunity to strengthen the customer's own change management policies.

Customer Complaints and Grievance Redressal Mechanisms should be in published form, from the Service Provider (CSP) and need not be prescribed/mandated. These could include 24x7 call center, chat and web support, mechanism to raise the complaint/ticket for the grievance along with an escalation matrix for raising the level, if required.

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.

BIF Response:
Security is often the top concern for government departments and agencies considering the move to cloud-based services. Government departments and agencies need to reassess the traditional IT network firewall protection principle in recognition that the movement of data increasingly crosses the
IT network firewall. This means building security into data, applications, infrastructure, and hardware layers (i.e., adopting end-to-end layered security) rather than relying on the assumption that the IT network firewall is the first and last line of defense.
Responsibilities regarding the managing of risks between the customer and the cloud provider will vary depending on the cloud delivery model (For e.g. end users have less control over risks in SaaS model compared to IaaS model). It is neither reasonable nor realistic for the government to effectively mandate outcomes across these various models given that they vary widely. Contractual responsibilities and compliance boundaries will vary equally.
It must be stated that unlike the presumption made in the TRAI CP , an on-premise system that is connected is probably at the same level of risk as data or processes stored in the cloud . Data Security may be more effectively managed by a CSP than by the IT department of an SME. Keeping data and processes offline can aggravate data security, reliability and availability issues.

It must be understood that there are different approaches to deploy cloud services in a public, private or a hybrid cloud model. Using cloud services does not necessarily imply use of a public or a multi-tenanted cloud. The customer's evaluation of the risks and his ability to manage it in-house or his trust on the CSP determines whether data and processes should be stored in a

public or private cloud. Responsibilities regarding managing of risks between the customer and the cloud provider will vary depending on the cloud delivery model. It may be noted that customers have less control over risks in a SaaS cloud model as compared to a IaaS model . In the latter , the user may be responsible for ensuring that the Operating System(OS) is patched for security vulnerabilities while in the former, the user has no exposure to the OS at all.

BIF believes that it is neither realistic nor reasonable for the Govt to effectively regulate the outcomes across various models given the wide variance amongst the models besides variance in contractual responsibilities and compliance boundaries

As regards to security, there are several cloud implementations where storage and transmission of data are protected in a way that only the customer and not the cloud provider/vendor have access to the keys . Therefore the assumption made in para 4.6 of the CP about data streams being visible to the CSP in an unencrypted form is not always true. Lawful interception to such data will also be dependent on how the data is protected. For business critical data, the CSPs should offer data encryption for data in storage and data in transit, for which various technologies are available.

Conformance to Cloud Computing Security and Privacy standards ISO27017 and ISO27018 and ISO27001 should be recommended. From physical security perspective, the following should be mandated viz.

-Facilities manned 24x7x365 days

-Digital Video Surveillance record for 90 days to be retained

-Multi-part authentication at all entrances: smart bridge, biometric scan, etc

-Server Room access strictly restricted to authorised employees and escorted contractors/visitors

-Employees to go through a " On Boarding Process" and stringent access request procedure

-Revalidation of restricted employees once in every quarter

-Rigorous off boarding procedure

Besides the CSP should be required to share audit reports on need basis and permit Customer visits to the Data Center , if required.

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

BIF Response:

Security models and assumptions need to evolve as governments adopt cloud computing. To address such security needs in the move to cloud computing, proactive government departments and agencies are working with industry to define security standards and implementation approaches (e.g., encryption, authentication, authorization, and geo-location capabilities).
Initiatives such as the European Union Agency for Network and Information
Security (ENISA) aim to improve the public sector's understanding of the
security of cloud services and the potential indicators and methods that can be used during service delivery.
Exit criteria should be defined upfront so that there are no surprises viz. requirement to erase data footprint in the CSPs' cloud and the cost ceiling to transfer date from the CSP back into the organisation

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

BIF Response:
As customers transition their applications and data to cloud computing, it is important that the level of service provided in the cloud environment be comparable to the service provided by their traditional IT environment. Failure to properly migrate applications to cloud computing could ultimately result in higher costs and potential loss of business, thus cancelling any of the potential benefits of cloud computing.
This section provides a prescriptive series of steps end users should take to ensure successful migration of existing applications to cloud-computing:
1. Assess your Applications and Workloads
2. Build the Business Case
3. Develop the Technical Approach
4. Adopt a Flexible Integration Model
5. Address Security and Privacy Requirements
6 .Manage the Migration A key component of successful cloud uptake is ensuring consumer trust in the privacy and security of their data stored on the cloud. In most cases, security and privacy are contractually ensured, and based on the customised arrangements required by a customer. As a result, there is no need for further regulation. At the same time, transparency in cloud offerings should be ensured in order to engender consumer trust.

Elements of such a framework should include full disclosure of countries where data is likely to be located, including those from which data access can occur (e.g. in case of remote maintenance); as well as full disclosure of a cloud supplier's subcontractors and transparency in contractual obligations (safety, responsibility, confidentiality, reversibility, data protection).

To reinforce security and trust in the cloud, transparency could be achieved by setting up a voluntary checklist of cloud contracts possible requirements viz

-List the countries where data is likely to be located including those from which data access can occur (viz. in case of Remote Maintenance)

-List of Cloud Supplier's sub-contractors; provider's contractual obligations (safety, responsibility, confidentiality, reversibility, data protection, etc)

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

BIF Response:
From the cloud service customer perspective, one of the significant areas of risk involved with cloud computing is associated with the division of activities and responsibilities between the cloud service customer and the cloud service provider. It is necessary to have a full understanding of who is responsible for which activities to ensure that there are no gaps which could lead to problems when using cloud services.
The cloud service provider and the cloud service customer are the most significant roles in the provision and use of cloud services while the cloud service partner is a party engaged in support of the activities of the cloud service customer and/or the cloud service provider.
Roles of Cloud Service Provider

- Cloud service operations manager
- Cloud service deployment manager
- Cloud service administrator
- Cloud service business manager
- Customer support & care representative
- Inter – cloud provider
- Cloud service security &risk manager
- N/w provider.

In general, there should be a shared security model. Both CSP & Customers should be responsible for cloud security . Customers should be responsible for 'security in the cloud ' which includes security of the data, applications, operating systems, network and firewall configurations.CSP should be responsible for ' security of the cloud '. This shall include all computing and storage resources, databases, networking and other components Security has three aspects viz. Confidentiality, Integrity and Availability. While Confidentiality & Availability should be the responsibility of the CSP, Integrity should be shared responsibility.

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?

BIF Response:
Some of the top security concerns pertain to
a) Physical location of data especially if they are located in another country because laws of the host country apply to the machine and the data residing on it. That becomes an issue if the host countries do not have adequate laws to protect sensitive data or if the host nation becomes hostile.
Primary location of data and any backup location must be known to ensure that these laws and regulations are followed. For example, in EU , it is mandatory that data controller must inform individuals that data will be sent and processed outside of EU, if required. The Data Controller and the end processor must have contacts approved by the Data Protection Authority in advance, though this will have different levels of difficulty depending on the region that is processing data.
It is therefore necessary to ensure that any cloud providers that are outside the jurisdiction have adequate security measures in place. This includes primary and backup location as well as any intermediate locations if data is being transferred between jurisdictions.

Any information stored in the cloud eventually ends up on a physical machine owned by a particular company or person located in a specific country. A Cloud Provider may without notice to the user, may move user information from one jurisdiction to another or even sub-contract cloud services. Legal location of information placed in a cloud could be one or more places of business of the cloud provider, location of the computer on which information is stored, location of communications that transmits information from user to provider and from provider to user, location where user has communicated or could communicate with provider or possibly other locations.

Laws of user's country may restrict cross-border transfer or disclosure of certain information. Data on cloud maybe subject to third party /Govt. access without user's knowledge. Data stored in another country maybe more accessible to Govt. under local laws. In sync with privacy of data shared with the cloud is whether such information is permissible to be shared under legislation of user's country or transferred outside the country's borders. For example in the US, there are laws that restrict disclosure or sharing of certain information viz. tax returns, health records, etc. The pertinent questions that arise are what the level of disclosure is and whether using cloud to store information amounts to it being disclosed.

CSP should share the information of their data location policies with the User. Movement of data should be protected both by contractual provisions as well as prevailing data privacy laws. Government should not limit data location or restrict cross border data flow as they limit the efficiency and efficacy of cloud services and restrict user choices.

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?

BIF Response:
While existing laws do cover some legal issue thrown up by Cloud Computing, they don't contemplate scope of Cloud Computing services and resultant enlargement of the scope of the issues. Consequence of this is that current laws may not possibly be able to facilitate Cloud Computing and there is need for specific regulation whereby any emergent issues could be dealt with directly.

Regulations need to be evolved for Cloud Computing in India for Regulation of Investigatory Powers, Regulation on Stored Communication, Mandatory guidelines for National Security for Cloud Operation, Lawful interception & monitoring by Lawful Enforcement Agencies, State Privacy Laws, Fair Credit Reporting Act, etc.

Lawful interception is an extremely important aspect of any communication/information transfer. Lawful Interception by a Law Enforcement Agency is an established and transparent method of letting Govt. protects its boundaries, integrity and sovereignty in addition to National Security. The Govt. will have to ensure strict and vigilant interception system in Cloud Computing environment so as to meet the said requirements.

Older methods of Lawful interception need to be reviewed in the light of the new developments in the cloud viz

-Machines & data are no longer physically in one place or within the same national boundaries
-Encryption & Data security need to be far stronger and of international standard
-End companies have to sign deeper and more stringent End User Agreements with customers that previously never covered data as data was local and software was able to process it locally.

Following measures can be incorporated to channelise a legal framework for Cloud Computing

1. Customised Agreements for Data

Cloud Service Customers & suppliers could seek to legitimise international transfers on the basis of adapted version of the new model clauses. Compared to the new model clauses, tailored data processing agreement should not reduce contractual safeguards, should incorporate same description of transfers and detailed security measures. This would enable room for both customers and suppliers to carefully incorporate various clauses which are contract specific.

2. Legal Framework for Data Ownership

Cloud Service Provider must safeguard integrity of data and guarantee client ability to easily migrate its data and guarantee client the ability to easily migrate its data and records to another hosting service in case of unsatisfactory performance . This should be done after complete deletion of all the data in the current cloud.

3. Cross Border movement legal framework

Analysts & techno-legal experts have offered a solution that cyber space must have its own set of jurisdictional rules thus erasing geographical boundaries.

4. Binding Safe Processor Rules (BSPR)

BSPR is a global code of practice for data processor's organisation based on EU privacy standards. In medium to long term, suppliers can address customer's concerns on the basis of BSPR which is a self regulatory solution for data processors. They set out appropriate adequacy standards and can be tailored to data protection practices of Cloud Supplier standards. These standards are applied by Cloud supplier or processor to customer's or controller's data and are uniformly applied across supplier's organisation. BSPR enables customers to easily comply with their data protection obligations and eliminates the need for model contracts.

5. Multi-jurisdictional issue legal framework

It helps overcome problems of multiple jurisdictions. One of the possibilities maybe to mandate Cloud Service providers host data centres only in India. Another alternative is to impose restrictions on cross border movement of some critical information viz. tax returns, financial transactions, health records, etc.

6. Adequate penal measures

Where law stipulates certain precautions to be taken by ISP, vendor and intermediary with respect to data storage, transfer a& processing, it fails to enumerate any stringent penal action against those who violate these precautions. Punitive measures and fines defined are too meagre to ensure proper protection of data. Personal & sensitive data has to be maintained with utmost confidentiality and trust of information provider must be safeguarded. Where highly sensitive data is being handled, law may also suggest an imprisonment term (depending on gravity of crime) in addition to the time prescribed. For repeated contravention, licenses of the service providers may be revoked.

Govt. could probably introduce some form of license /operational restrictions on Intermediary Service Providers. Complying with new rules under amended IT Act 2000, requires providers of sensitive information to verify information which can become onerous given that data maybe

held in fragmented corners of the cloud. The laws need to be reviewed and new policies should be introduced to effectively and efficiently deal with matters involving confusion with respect to basic & highly important issue of jurisdiction.

Government should leverage existing mutual legal assistance treaty (MLAT) agreements and INTERPOL to address lawful intercept requirements beyond national boundaries. If the system architecture permits decryption to take place (where vendor/operator holds the key) , then only it should be mandated to the CSP to decrypt/provide access to data . Access requests should be backed by proper legal authorisation. Encryption used by corporate enterprises intended to create a secure private network for corporate communications should be preferably not be subject to requests for access to unencrypted data

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

BIF Response:
In India, as cloud services are at an emerging stage, any restriction in the scope may hamper the expansion of these services. All individuals, organizations including telcos and non-telcos should be allowed to utilize the cloud platforms for all their respective database and information without any restrictions. Thus, Cloud solutions should not require any separate licensing or registration requirements. These services should be treated as other services offered over the internet and should not be treated in a differential manner.

Cloud Computing may be treated like Internet services and hence not be subject to a separate law or licensing or registration requirements. It is in the best interest of the industry and the consumer that there should be no unnecessary hindrances to free flow of data. In fact BIF is of the opinion that businesses should have the right to choose where they store their own data. The regulatory environment should promote the ability for companies to autonomously make decisions on data localisation when it is beneficial to their specific business. BIF recommends avoidance of any forced data localisation requirements in India and globally. Such artificial restrictions on data movement make it more difficult to implement best practices in data security, including redundant geographic storage of data and usage of distributed architecture based security solutions.

Also such restrictions shall compel companies to increase their dependence upon local data centers that lack sufficient capacity, upgraded hardware or experienced security personnel to counter intrusions and detect signals associated with potential breaches. Such restrictions also deprive businesses of employing the best technical solutions for security protection because of the obligation to store data in a specific geographic area. Besides, centralised storage of data

increases the probability for hacking or surveillance as the efforts to access one single data centre is much less than several ones, in the case of a cloud based system

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?

As discussed above, cloud service providers should not be asked to submit to the territorial jurisdiction of India for the purpose of lawful access of information, i.e., no mandatory/forced localisation policies should be pursued by the government. Where data is stored is an issue that must be the prerogative of each service provider, based on the requirements of its business model and/or specific customer requirements. This is an essential component of evolving a framework that encouraged date centre deployment in India.

i. Data localisation policies should not be mandated

As discussed above, data localisation when mandated by law can have a number of deleterious effects on global competitiveness and private investments. Localisation policies are not only unjustified but also make it more difficult to implement best practices in data security – including redundant geographic storage of data and the usage of distributed security solutions. Businesses would be deprived from the ability to deploy the best technical measures available to protect security, only because they would have the obligation to store the data in a specific geographic area.

Storing data in a single centralized location can also offer a more attractive target for hacking or surveillance, because the efforts to access or compromise one single data centre rather than several ones are limited. Decisions including where data may be stored must be left up to cloud service providers and their respective clients. Government interference would only pose a barrier to cloud adoption.

ii. Trans-border data flows should be encouraged

Trans-border data flows form a key component of the economic and strategic benefits cloud computing can bring to the Indian economy. Any geographical restrictions on data flows would impede cloud computing from resulting in economies of scale and slow down the adoption/penetration process. Ultimately, this would impact India's economic benefits from cloud computing, and reduce its competitiveness on the global stage – creating an island of restriction in what is otherwise a borderless internet.

In addition to economic considerations, restrictions would create a 'balkanised' version of the internet and break its open nature. As a result, no restrictions on data flows should be implemented by the government in any direct or indirect form.

iii. National Security concerns are adequately addressed by existing regulation

At the same time, it may be noted that there exists sufficient regulation in the form of the Indian Information Technology Act framework which empowers the government to carry out interception, monitoring, and decryption of information passing through computer resources in India. Where, information is sought from cross-border entities, sufficient procedures exist in the form of well-established principles and mechanisms of international law governing international co-operation between countries for enforcement of domestic laws, such as under Mutual Legal Assistance Treaties (MLATs) entered into between different countries.

If there is any aspect of this process that is lacking, it is in terms of levels of awareness for law enforcement and other agencies. The government may seek to improve the efficacy of these processes through training and capacity building. Additional regulation would only create barriers to adoption, and decrease India's competitiveness in the global field.

As regards to compliance with Indian laws by online CSPs located outside the country , the IT Act 2000 explicitly states that it is applicable even where any offense or contravention is committed outside India irrespective of nationality. However disclosures of account records in such cases are in accordance with their terms of service and applicable law.

Conflict of laws create an increasingly chaotic legal environment for online CSPs , restrict the free flow of information & data and leave private businesses often in a conundrum as to which country's laws they would be violating. Despite the limitations stemming from conflicts in law, it is seen that existing non-content and emergency disclosure processes have worked effectively to facilitate cross border disclosures.

Additionally, it is important to recognise well-established principles and mechanisms of international law govern international co-operation between countries for enforcement of domestic laws such as Mutual legal Assistance Treaties (MLATs) and for concerned agencies to keep discussing opportunities to improve these processes and enhance mutual cooperation.

In summary, BIF believes that the same framework that applies for existing internet services, should be applied for the CSPs.

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.

BIF Response:

The promotion of cloud deployment and establishment of data centres in India are linked to the levels of investments made by private entities within India. In this regard, what is required is a policy framework manifesting certainty, security, and transparency to ensure that investments are protected, and maximum freedom provided for them to generate value.

The government should seek to adopt a facilitative framework which privileges adoption, and growth in the sector. Burdensome and mandatory regulations would stifle cloud deployment and lead to India potentially foregoing a critical growth opportunity.

A key target of creating a more conducive environment for cloud solutions should be the improvement of physical cloud infrastructure including in relation to ensuring consistent power and water supply. In addition, the government must take urgent measures to ease business process for entities seeking to enter the Indian market. On average it takes 67 days on an average for a company to obtain an electricity connection in India, as against 3 in Japan. Taking steps to address these shortcomings would provide a significant boost to the appeal of India as an investment destination for data centres.

The policy requirements for India should begin with developing a comprehensive and systemic framework for data centres. The motivation should be to create an enabling environment for private players to enter the data centre market and to meet the growing needs of data management in India. In this regard, the government should encourage voluntary adoption of standards and best practices, without seeking to interfere by way of regulation. This is to ensure that the Indian economy remains competitive and is given every opportunity to emerge as a leading cloud hub.

India has a great opportunity for developing a regulatory regime that incentivises private equity and investments in establishment of data centers in the country. Sop, a conducive regulatory and policy ecosystem that comprehensively addresses such needs with transparency, certainty and long term stability and assurance is necessary. Currently the regime is extremely uncertain and the requirements are subject to bureaucratic and regulatory approval.

The policy and regulatory requirements should begin with a comprehensive and systemic framework for data centers. The Policy and regulatory environment should be such so as to encourage private players to enter the data center market and meet the growing needs of data management in India. It is a given that the data center market is capital and technology intensive which will result in technology and capital inflow from market leaders. This is likely to make a positive impact on the Indian economy.

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?

BIF Response:

IT resources and services that are abstracted from the underlying infra-structure and provided on demand and at scale in a multitenant and elastic environment offers the ability to break down IT silos with their inefficiencies, high costs, and ongoing support and maintenance issues while meeting increasing user demand for cost-effective, innovative service on demand across network, computing, and storage resources.

Cloud computing is justifiably called a transformational model for the enterprise. It transforms IT and the data center as we have known it: dedicated consumption, lengthy hardware procurement, manual addition of new services, manual repair of system failure, provisioning in months, and incremental capital expenditures. Cloud computing can provide flexibility, efficiency, and democratization around resource allocation, resulting in agile IT service delivery—provisioning in minutes and time to market reduced by more than 50 percent—and cost optimization with higher server and storage utilizations, 50 percent reduction in capital costs, and 25 to 30 percent reduction in operational costs. And it affects the very way we do business—back office, supply chain, and governance, to name a few—and the way we engage with employees, partners, vendors, and customers and grow the business. Cloud computing profoundly transforms the way in which information and services are provided to and consumed by enterprise users: shared, self-service, scale on demand, automated recovery, provisioning on demand, and pays per use.

BIF wishes to re-iterate that it is in favour of removal of any restrictions to the free flow of data . It is of the opinion that data localisation should be prohibited both in India and globally as it makes implementation of best practices in data security difficult to implement including redundant geographic storage of data and usage of distributed security solution architecture. The Hybrid Cloud allows businesses to combine public cloud , private cloud and dedicated hosting by matching the right solution to the right job , thereby allowing the business to leverage the best that each model has to offer to build a most optimum solution that perfectly matches the business needs.

For example, the public cloud could be used for non-sensitive operations and for heavy, spiky and unpredictable workloads the private cloud could be used for Business critical operations that require specific settings for specific workloads or for those cases that require greater levels of security.

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?

BIF Response:

The data centre industry's needs are unique from each other so a conducive regulatory and policy ecosystem that comprehensively addresses such needs with transparency, certainty and assurance is necessary. At present, an investor in
the data centre market will not be in a position to invest with certainty or to avail governmental incentives or schemes as the applicability requirements are subject to bureaucratic and regulatory approval.

Indian telecom laws follow a different approach as compared to the International Laws. The challenge is to expand telecom and internet density and introduction of new technology and services. The authorities must devise protocols for third and fourth generation networks which are the need of the hour for ensuring a comprehensive and systemic framework for data centres. Such policy should be driven by a motive to create an enabling environment for private players to enter the data centre market and to meet the growing needs of data management in India.

The challenges that India faces are:

-Lack of sufficient infrastructure

-Complicated regulatory mechanisms and bureaucracy

Additional challenges related to data centers are :

-Requirement of Huge Space Capacity

-Power

-Cooling provisions

Cost is also one of the primary challenges to data center development and growth in India. Energy makes up for the lion's share of the cost, almost to the extent of 75%. Additionally energy usage in this sector is growing at a high rate and this is likely to continue. The growth in demand of energy and cost of generation of energy is also on the higher side. Besides energy needs, data centres require an enormous volume of water to cool high-density server farms , thereby making water management a growing priority for data centers.

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?

BIF Response:

Data centre incur one-time and recurring taxes that have a significant impact on long-term costs for any data centre.

The capital-intensive nature of a data centre attracts relatively high sales taxes and property taxes. India can adopt such data centre-specific tax and duty incentives that will encourage investors to operate here. Where to locate the assets and the people associated with delivering global data content and services is a defining tax consideration — in terms of both direct corporate tax rates and indirect sales taxes. Friendly tax jurisdictions play a big factor in choosing a place for establishing a data centre and complex tax jurisdictions do just the opposite. Tax incentives for building infrastructure for large data centres and cloud services within the country should be allowed to ensure data security as well as to have a big network of large software products companies within the country. The recent Budget announcement of reducing corporate tax rate and reduction in the tax rate on Royalty and Fees from Technical services is much appreciated which would surely give a lot of boost to the industry. Similarly the eCommerce firms are also expecting implementation of crucial tax incentives for building data centres and cloud services within the country.

As discussed above, a number of emerging economies have taken a lead over India in adopting frameworks which facilitate and encourage cloud computing. Therefore, India must take every possible step so as to not miss out on a critical growth opportunity.

Data centres are capital-intensive establishments which entail both one-time and recurring costs which include sales, property taxes, electricity tariff, stamp duty charges, import duties on equipment sourced from outside India and multi-jurisdiction tax implications. At the same time, the developmental effects of data centres are well-known with there being well-defined benefits to local employment, GDP, and productivity resulting from the establishment of data centres in a region. Therefore, tax incentives may be an avenue to maximise long-term development and growth potential at the cost of short-term revenue losses.

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

In this regard, the Indian government should provide data centre-specific tax and duty incentives that will encourage investors to operate in India. Additionally, benefits may be provided in the form of discounted electricity/water tariffs, and financial incentives to adopt eco-friendly energy practices. Where to locate the assets and the people associated with delivering global data content and services is a defining tax consideration — in terms of both direct corporate tax rates and indirect sales taxes. Friendly tax jurisdictions play a big factor in choosing a place for establishing a data centre and complex tax jurisdictions do just the opposite.

Data Centers incur one-time and recurring taxes that have a significant long term impact on the overall costs. The Capex intensive nature of a data center triggers relatively high Sales Tax and other taxes. Further electricity tariff, stamp duty charges, import duties on foreign equipment and multi-jurisdictional tax implications further impact data center costing.

As in other developed countries viz. USA, it is suggested that India adopt data center-specific tax and customised incentives for data centers by way of partial or full exemption of taxes. This will attract investment into this area. Friendly tax jurisdictions play a big factor in choosing a place to establish a data centre.