EBG FEDERATION

**EBG FEDERATION RESPONSE TO TRAI CP CONSULTATION PAPER ON CLOUD COMPUTING**

**Preamble**

According to Gartner "Public cloud services revenue in India will reach $731 million by the end of 2016. The 2015 Public Cloud Services revenue was driven by high growth rates in key market segments, such as Cloud Infrastructure as a Service (IaaS), Cloud Management and Security, and Software as a Service (SaaS). Gartner also predicts high rates of spending on cloud services in India to continue throughout 2019 when the market is expected to reach $1.9 billion.

The benefits of adopting cloud computing can be illustrated by a 2011 survey for the European Commission which shows that as a result of the adoption of cloud computing 80% of organisations reduce costs by 10-20%. Other benefits include enhanced mobile working (46%), productivity (41%), standardisation (35%), as well as new business opportunities (33%) and markets (32%).

EBG Responses to Questions are as follows:

Q1. 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.

**EBG Response:**

**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. 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**

Q2. Please indicate with details how the economies of scale in the cloud will help cost reduction in the IT budget of an organisation?

**EBG Response:**
**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.

EBG FEDERATION

**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 an IT systems administrator has to spend 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 organisations. Overall reduction of computing costs can also greatly reduce barriers to market entry for organisations, allowing for greater levels of innovation and growth. Cloud computing allows organisations to scale more effectively because they can buy computing services as needed instead of making large upfront investments in data center infrastructure.**

2nd Floor, Building No. 6, Okhla Industrial Estate, Phase 4, Okhla, New Delhi 110 020, INDIA
Ph.: 9811418874 E-mail : gm@ebgindia.com
Website: www.ebgindia.com

***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.

Q3. 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?

**EBG Response:**

Cloud computing is becoming a game changer for Small-Medium Enterprises (SMEs) by offering scalable infrastructure and capabilities available as services. It is a paradigm where computing resources are available when needed, and you pay for their use in much the same way as for household utilities.

For small businesses, outsourcing IT to the cloud lowers the need for specialist skills and frees managers to concentrate on the core business. It may cost slightly more than in-house IT, but this is often outweighed, as it can sometimes enable a small company to take a "big company" approach to problems by increasing efficiency.
Cloud computing isn't just for data, you can also use it to run applications and software remotely, without being tied to one computer.

- The first level of cloud services is called Infrastructure as a Service (IaaS). It works by providing virtual hardware, such as computers, raw processors, storage software

platforms and so on. Instead of being physically based in an office, employees can access their data via the internet.

- The second level, known as Platform as a Service (PaaS), provides all the resources necessary for small business owners to create their own software and programmes. Usually this will include an operating system, programming environment, database, and web server. This can save you the cost of storing and investing in the hardware and software which would otherwise be necessary.
- The third level available is Software as a Service (SaaS), which provides you with software and programmes which are available and ready to use. You can run them remotely, without having to go through lengthy installation processes and worry about how your hardware will cope with the application.

While IaaS and PaaS will have some value to businesses large enough to have their own computer installations, it is SaaS, with its access to applications that provides most value to small businesses.

**Q4. How can a secure migration path may be prescribed so that migration and deployment from one cloud to another is facilitated without any glitches?**

**EBG Response:**

A system that involves cloud computing typically includes data, application, platform, and infrastructure components, where:

- *Data* is the machine-processable representation of information, held in computer storage.
- *Applications* are software programs that perform functions related to business problems.
- *Platforms* are programs that support the applications and perform generic functions that are not business-related.
- *Infrastructure* is a collection of physical computation, storage, and communication resources.

The application, platform, and infrastructure components can be as in traditional enterprise computing, or they can be cloud resources that are (respectively) software application programs (SaaS), software application platforms (PaaS), and virtual processors and data stores (IaaS).

Non-cloud systems include mainframes, minicomputers, personal computers, and mobile devices owned and used by enterprises and individuals.

Data components interoperate via application components rather than directly. There are no “data interoperability” interfaces.

Portability and interoperability of infrastructure components are achieved by hardware and virtualization architectures. The interfaces are mostly internal to the IaaS and infrastructure components shown in Data, Applications, Platforms, and Infrastructure. The interfaces exposed by these components are physical communications interfaces: these are important, but are the same as for traditional computing. For these reasons, infrastructure portability and interoperability are not discussed further in this Guide.

The main kinds of cloud computing portability to consider are *data portability*, *application portability*, and *platform portability*. These are the portability respectively of data, application, and platform components.

*Application interoperability* between SaaS services and applications, and *platform interoperability* between PaaS services and platforms are important kinds of cloud computing interoperability to consider.

Applications can include programs concerned with the deployment, configuration, provisioning, and operation of cloud resources. Interoperability between these programs and the cloud resource environments is important. This is *management interoperability*.

Applications can also include programs such as app stores (for applications), data markets (for, e.g., openly available data) and cloud catalogues (e.g., reserved capacity exchanges, cloud service catalogs) from which users can acquire software products, data and cloud services, and to which developers can publish applications, data, and cloud services. In this Guide, all such programs are referred to as *marketplaces*. *Publication and acquisition* of products is performed by platforms, including PaaS services, that interface to the marketplaces. This is the final important cloud interoperability interface.

The cloud computing portability and interoperability categories to consider are thus:

- Data Portability
- Application Portability
- Platform Portability
- Application Interoperability
- Platform Interoperability
- Management Interoperability
- Publication and Acquisition Interoperability

In the context of cloud computing, interoperability should be viewed as the capability of public clouds, private clouds, and other diverse systems within the enterprise to understand each other's application and service interfaces, configuration, forms of authentication and authorization, data formats etc. in order to cooperate and interoperate with each other.

To date, most of the focus for cloud interoperability and portability standards has been at the IaaS layer although activity at the PaaS level is starting to accelerate. In addition, there are several security standards that enable and facilitate cloud computing interoperability even though they are not exclusive to cloud computing. Cloud Computing customers should determine the level of support for the following standards by prospective cloud service providers. Lack of support for these standards is likely to result in interoperability and portability challenges down the road.

**Q5. 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?**

**EBG Response:**

Establish sets of criteria that help customers analyze and evaluate migration and exit concerns before adopting and deploying cloud computing solutions. 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 recognising 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?

**Q6. 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?**

**EBG Response**

***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.

**Q7. 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.**

**EBG Response**

***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.

**Q8. 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?**

**EBG Response**

Cloud providers need billing systems that offer cost visibility, cost analysis, cost accounting and cost governance

**Cost visibility:** This refers to the ability to have near real-time access to the costs within a cloud computing provider's environment, including costs of the resources used, costs of any services provided to the cloud provider (such as external management and security systems), cost of the services provided to the cloud service consumer and other costs that may be germane to the provider.

**Cost analysis:** This is the process of taking the cost data that we're making visible to both the cloud service provider and consumer.

**Cost accounting:** This refers to the process of collecting, analyzing, summarizing and evaluating various alternative courses of action to determine if there were better, more cost-effective ways of leveraging the cloud service, based on the cost data gathered.

**Cost governance:** This is the ability for the cloud provider or cloud services consumer to institute cost-related processes and policies.

Requirements for cloud billing systems may vary depending upon the types of cloud services supported. Cloud billing systems should attempt to achieve the following:

1. Automated, multi-tenant cloud billing that can eliminate the time-consuming preparation of invoices that reflect the use of cloud services. Usage-based billing is complex, as it requires that a great deal of information be tracked during operations.

2. Self-service customer cost reporting that allows the provider to gain and increase customer trust by giving them anytime access to their downstream cloud costs. That way, even with the erratic cost patterns that emerge around cloud bursting, consumers can still predict future usage for both budgeting and governance purposes.

3. **Granular, time-stamped and auditable information about costs, tracked through all operations of a cloud service. This can quickly resolve billing disputes and eliminate costly discounts with accurate and auditable customer cloud usage and cost data. Everything is tracked, and everything is available**.

EBG FEDERATION

**Q9. What mechanism should be in place for handling customer complaints and grievances in Cloud services? Please comment with justification.**

**EBG 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 Availibility** - 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.

**Q10. Enumerate in detail with justification, the provisions that need to be put in place to ensure that the cloud services being offered are secure.**

**EBG Response:**
CLOUD COMPUTING SECURITY CHALLENGES

**OWNERSHIP OF CUSTOMER DATA**
When data resides in a cloud data center, it is important to clarify the ownership rights. There has been some concern that many providers' terms of use could appear to give providers intellectual property rights to the information they store or process, but studies by legal experts have found no evidence of this. However it is still important to clarify what rights—if any—are conferred on a cloud provider and what this means in practice. Encryption is one way to protect data that is being stored; however, this is not very useful when the data needs to be processed in the cloud. The customer should therefore make sure that data ownership is clearly defined and that the agreed terms are acceptable with respect to the customer's own security policy. It is also wise to clarify the ownership of data that is generated when the customer uses the service, such as trace logs, service usage patterns, Quality of Service information, and the like.

**USAGE OF CUSTOMER DATA**
Having clarified the ownership of customer data, it is equally important to control how providers can use the data. (An example is Microsoft's security, privacy and compliance information for O365 where it is stated that the address book data for Office 365 Small Business customers is used for marketing purposes.)

**DELETION OF CUSTOMER DATA**
Cloud services are by nature virtualized and duplicated, which is good for ensuring uptime and availability. Furthermore, the duplication is compounded by conventional backup processes performed in each data center. However, when the owner of a particular dataset wishes to delete it, this wide data distribution becomes a major challenge. It is difficult enough to ensure that all duplicated copies in each datacenter are erased, but ensuring that all backup media is expunged as well can take months. It is important to be aware that "deletion" does not always mean that data is actually erased; it is often only the pointers that indicate where the data fragments are located that are erased. Data deletion will therefore in most cases not be guaranteed by providers

beyond what is performed in a normal overwriting cycle of backup media. Provider commitments with respect to data deletion are important for cloud customers; not only when they are using the cloud service, but also after the contract has been terminated.

**FOG COMPUTING**

In the more recent "old days", one would buy a cloud service from a single cloud provider and that was it. However, the cloud ecosystem has evolved into a more diffuse fog of several cloud providers, resulting in less security visibility. A cloud service is likely to have many layers of abstraction that build on top of each other. Service providers adapt and compose several services into one, which is then offered to the cloud customers. Software-as-a-Service (SaaS) applications that an end-user interacts with are already often based on other providers' PaaS solutions, which in turn often run on yet other providers' IaaS offerings. Numerous combinations exist and more are expected to come. There will be chains of services and providers involved in the final service delivery.

From a security point of view this means that the cloud customer may, sometimes unknowingly, rely on many different parties, hence being subject to multiple points of failures, an increased attack surface and difficulties in verifying that legislation and internal security policies are being adhered to. Many of the security challenges in cloud computing are in part related to the complex provider supply chains in this ecosystem. To complicate things even further, services and data may be replicated horizontally among multiple providers. As a consequence, it is often extremely difficult to determine where data is being stored or processed at any one time.

**ACCESS CONTROL**

Access control management can be challenging enough within a single organization, but when moving services and data to the cloud, a new dimension is added. Cloud customers often fear unauthorized access to their data. Most providers have "backdoors" to their customers' data, and they often reserve the right to access it for maintenance, support and service reasons. It can be very difficult to know which roles and people have access to your data from the cloud provider side. For instance with Office365, database administrators employed at Microsoft reserve the right to have access to all the resources in all their databases, including their customers' data. Additionally, the Microsoft Operations Response Team and their support organization can access this data as well.

**MONITORING AND AUDITING**

Cloud providers may offer various options of monitoring data and processes related to their services; both from the provider's perspective of ensuring acceptable use, and from the customer's perspective of keeping track of what is happening in their corner of the cloud. This could include monitoring virtual machines in IaaS or monitoring behavior of running applications in PaaS and SaaS. Another example could be monitoring of network communication between virtual machines by network-based intrusion detection systems.

The big cloud providers have thousands, if not millions, of customers, and it would not be viable to allow any demanding customer to inspect a cloud datacenter as part of a service contract negotiation. Furthermore, due to the large number of other customers, allowing one customer unrestricted access to network and process monitoring data could jeopardize the confidentiality of other customers' data. However, many customers want to maintain a certain level of control, and some sectors are even required to do this by local regulations. Some of the smaller providers allow their customers to perform such on-site inspections as part of negotiation or annual reviews. In addition, accredited auditors may perform independent audits of cloud providers and their datacenters.

**STANDARDS AND CERTIFICATION**

Many customers rely on security standards as a way to ensure that an adequate level of security is attained; however, there is not yet any established standard that will fit all cases. There are currently more than 35 standards relevant for cloud security and it is unrealistic to expect a cloud customer to be conversant with all of them. Many cloud providers will typically claim that they are compliant or certified to a certain standard, but the ground work here for the customer is to make sure that this is of relevance to the kind of security they are looking for. Upcoming standards such as *ISO/IEC WD 27017 Code of practice for information security controls for cloud computing* and *ISO/IEC CD 27018 Code of practice for data protection controls for public cloud computing services* are expected to be completed late 2013, but with the rapid development of cloud technologies and the slow standardization progress, they might be outdated after just a short while.

**SECURITY TESTING**

With traditional software installed in your own premises it is not uncommon to run security tests in a controlled environment. When services are deployed in a public cloud, organizations tend to lose this possibility since many cloud providers do not allow their customers to do any testing on their own. Therefore, a typical check is to obtain information about the kind of security tests performed, and what are the results.

**INCIDENT MANAGEMENT AND RISK OF DATA LOSS**

There is no such thing as a perfectly secure system, and incidents are bound to happen from time to time. What is important to check is how incidents are dealt with, in the preparation, detection, reaction and investigation phases. In many cases it is up to the cloud provider to define *what* a security incident is, *when* or even *if* the costumers need to be informed about a breach, and *how* to notify them. Recent events have shown that providers often tend to keep quiet about security incidents for as long as they can, even though it is in the customers' interest to get informed as soon as possible.

In Europe it is expected that the new European Data protection framework, which is currently under a major revision, will include new obligations related to incident notification. This means that any cloud provider must establish mechanisms to notify regulators and affected companies and individuals of data breaches or information security incidents. The Cloud Security Alliance has recently released a whitepaper on the necessity for forensic functionality as a part of the Service Level Agreements (SLAs), such as requirements for notification, identification, preservation, and access to potential evidence sources.

**LOCK-IN AND PORTABILITY**

Today, many up-and-coming cloud providers are not making money due to the effort and investment required to gain a sustainable market share. Some are bound to be put out of business and we will probably see many new competitors entering the scene as well. An unstable market is to be expected in the coming years as the cloud ecosystem grows into adulthood, so before deciding on a cloud service provider, it is important to have an idea on how to migrate to a different cloud provider should it be necessary. Data lock-in is one of the top concerns organizations have towards cloud computing. The typical checks here are related to how much time one has to migrate the data, whether there are any tools or APIs for exporting the data, the format which the data will be recovered into, and how the original data is going to be deleted.

**ISSUES WITH REGULATION**

Actors who have to abide by the European Data Protection Directive (DPD) have to be conscious about whether they store personal data in the cloud, and if so, where that data is transferred. The directive prohibits transferring of personal data to jurisdictions that do not offer sufficient protection of such data, but determining which countries it would be okay to transfer data to is not something that is easily accomplished by the average cloud customer. Thus, the short-term solution for many European cloud customers is to request that their data—including back-ups and logs–be stored only in European data centers. However, even when a cloud provider agrees to such terms, it may not be easy to ensure that no undesired data transfers take place. This is again due to the complex provider chain, for instance where one cloud provider, whose datacenters are all in Europe, somewhere down the line uses services from another cloud provider that also has datacenters in India. It is currently difficult to verify data export restrictions in long cloud provider chains.

Another issue with regulation is related to the definition of "data controllers" and "data processors" in the DPD. Cloud customers who transfer personal data to cloud infrastructures will become data controllers and will thereby need to follow strict requirements when engaging cloud providers to process the data. The definition of "processing" in the DPD is very broad and includes any operation on data in a cloud infrastructure, including collection, storage or disclosure. In most cases, storage providers (IaaS) do not have any way to control what kind of data their customers upload to their data centers. They therefore risk becoming data processors (involuntarily and possibly also unknowingly), and thereby subject to the strict DPD regime, if their customers upload personal data to their data centers. A "data processor agreement" must therefore always be established between the cloud customer and the cloud provider before personal data is transferred to the cloud.

When moving to the cloud, a security cautious customer would typically worry about issues such as:

- How will security be handled and who will be responsible for what?
- Which certificates and standards are best for cloud security?
- Where should I look to find a service that fulfills my security needs?
- How can I compare the security level of two otherwise equal services?
- What kinds of security guarantees should be included in the contract?

"Security" is a complex, slightly ambiguous and imprecise concept. It can be and probably is interpreted in many different ways. Security can for instance map to and concern one or more of the following areas:

- Data protection (and information classification, data encryption,etc.)
- Data access
- Identity management
- Authorization
- Authentication
- Data privacy
- Data integrity
- Accessibility
- Operations

Setting Standards and providing certifications are one way for helping organisations choose secure Cloud Services.

Some of the most important issues for certification are:
Data storage location (one aspect of privacy), cloud data centre infrastructure, cloud provisioning process and interoperability/reversibility

Secondly, make sure that Cloud Computing stakeholders (users, customers and providers) are made aware of existing standards and certification programs.

**Q11. What are the termination or exit provisions that need to be defined for ensuring security of data or information over cloud?**

**EBG 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.

**Q12. What security provisions are needed for live migration to cloud and for migration from one cloud service provider to another?**

**EBG Response:**
Portability is an important consumer concern. While there may be no contractual barrier to switching from one cloud computing service to another, providers could use proprietary formats or employ technical obstacles to make it difficult to do so. For instance, a consumer might be required to select each file individually to download. For consumers who have spent years uploading data, this could effectively make the service non-portable, locking them in and threatening competition.

Interoperability is a related issue; unless standardized data formats are used, it might be hard for consumers to use data that they have customized on one service with another service. Cloud computing services should not interfere with consumers' ability to move their data to another service or to use their data in an interoperable manner with other services.

Consumers may have no confidence about the security of cloud services, however, unless those services are required to meet adequate security standards and to be independently audited on a regular basis to ensure compliance. Cloud computing services should provide consumers with information about their security. In addition, cloud computing services should provide consumers with the means to safeguard their data through tools such as encryption for which only the consumers themselves have the keys. While the location of the servers that cloud computing services use can actually enhance the protection of consumers' data, cloud computing services should not be allowed to exploit the physical locations of their servers in order to limit consumers' rights concerning the privacy and security of their data.

Transparency is a guiding principle for all consumer transactions: consumers cannot make informed choices without understanding exactly what is being offered and on what terms.

Another concern is the fairness of terms of service. Many consumer contracts, including those for cloud computing, are one-sided agreements in which the providers disclaim any liability if things go wrong, reserve the right to change terms unilaterally, and require that disputes be resolved through privately-operated arbitration that is binding on consumers. Unfair contract terms for cloud computing services should be prohibited. For instance, cloud service providers should not be allowed to disclaim responsibility if they lose consumers' data, or to suddenly terminate services without notice and giving consumers sufficient time to retrieve their data.

Furthermore, terms of service should not require consumers who use free services to agree to a lower level of protection than those who pay or require that consumers give up the right to take legal action to resolve disputes. Cloud computing services should provide consumers with clear information on redress and compensation in the event that their data is lost, shared or stolen and with easy- to- use methods for making such claims.

**Q13. What should be the roles and responsibilities in terms of security of (a) Cloud Service Provider (CSP); and (b) End users?**

**EBG 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 reprenstative
- Inter – cloud provider
- Cloud service security & risk manager
- N/w provider.

**Q14. 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?**

**EBG Response:**

The European Union Agency for Network and Information Security (ENISA) has the following guidelines which may be of use since research has been done by European Commission for the Digital Market:

*Appropriate actions on contract terms can also help in the crucial area of data protection. As noted above, the proposed Regulation on personal Data Protection will guarantee a high level of protection for individuals by ensuring continuity of protection when data is transferred outside the EU and EEA, namely through standard contractual clauses governing international data transfers and establishment of the necessary conditions for the adoption of cloud-friendly binding corporate rules. These changes will ensure the EU data protection rules cater for the geographical and technical realities of cloud computing. The Commission will by end 2013:*

- *Develop with stakeholders model terms for cloud computing service level agreements for contracts between cloud providers and professional cloud users, taking into account the developing EU acquis in this field.*

- *In line with the Communication on a Common European Sales Law, propose to consumers and small firms European model contract terms and conditions for those issues that fall within the Common European Sales Law proposal. The aim is to* ***standardise key contract terms and conditions, providing best practice contract terms for cloud services*** *on aspects related with the supply of "digital content".*

- ***Task an expert group set up for this purpose*** *and including industry* ***to identify*** *before the end of 2013* ***safe and fair contract terms and conditions for consumers and small firms****, and on the basis of a similar optional instrument approach, for those cloud-related issues that lie beyond the Common European Sales Law .*

- ***Facilitate Europe's participation*** *in the global growth of cloud computing by: reviewing standard contractual clauses applicable to transfer of personal data to third countries and adapting them, as needed, to cloud services; and* ***by calling upon national data protection authorities to approve Binding Corporate Rules for cloud providers****.*

- ***Work with industry to agree a code of conduct for cloud computing providers*** *to support a uniform application of data protection rules which may be submitted to the Article 29 Working Party for endorsement in order to ensure legal certainty and coherence between the code of conduct and EU law.*

**Q15. 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?**

**EBG Response:**

The most fundamental need for LEAs is to be able to identify and communicate with the CSPs responsible for the communications involving specific targets. Cloud environments are especially challenging because the relevant CSP's are often not subject to registration, regulatory or CSP partnership needs that facilitate discovery of their identity(ies). Furthermore, the responsible providers' relationships are often complex. For example, relationships are layered, where an application service provider with the direct customer relationship uses a Software-as-a-Service provider that aggregates Infrastructure-as-a-Service resources at a data centre.

The introduction of Cloud services may increase the complexity and challenges for Lawful interception. The variations of Cloud services (e.g. IaaS, CaaS, PaaS) may introduce new or more complex business models and relationships amongst CSPs/C(L)SPs.

CSPs may protect/secure subscribers data through encryption or subscribers of Cloud services may encrypt the data prior to transferring it "into the Cloud". End-user encryption usage may actually increase with Cloud services as this ensures a subscriber of exclusive control over their data and prevents CSPs from accessing their subscriber's data for their own uses (e.g. data mining). **CSP's or subscribers who initiate encryption must provide unencrypted data (or if they cannot remove the encryption), must provide the LEA with the keys for decryption** and other information needed to access the information where such keys are available to the service provider.

**Q16. 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.**

**EBG Response:**

Providing licenses and requiring registrations will increase administrative workload for both stakeholders, CSPs and Government of India. It may also prove a deterrent for development of Cloud Services.

We have talked of Standards and Certifications for Cloud Services to facilitate users comfort and confidence levels. Government should play the role of facilitator rather than regulator.

**Q17. 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?**

**EBG Response:**

Ex Ante Laws will be going against the framework which applies to the internet.

As suggested in Response 16, CSP's should be guided by Standards and Certifications, efforts to keep both Users and CSP's informed of latest certifications and maintain a dialog with all stakeholders for fairness of business.

In case of a criminal activity then the Law of the land should apply, on appropriate investigative agencies providing sufficient evidence towards the same. Deterrents through ex post punitive measures may be the suggested way

**Q18. 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.**

**EBG Response:**

Government leadership can provide a more stable environment in which to consider the risks. Auditing standards, transparency and reporting requirements and imposition of liability on CSPs and subcontractors for breaches are all potentially useful means of balancing stability and growth.

Currently, there are significant challenges for India to become a hub for large Cloud data centers due to, inter alia, the quality and reach of the data networks, broadband and power grid capabilities

With a literacy rate of 61 percent and challenging statistics in terms of school attendance, the general awareness regarding new technologies in India is a big challenge. This is complicated by the diversity of local languages present in India.

Currently, most Cloud services are provided by CSP's outside India and hence do not provide interfaces in Indian languages. Regulations and policy level incentives are needed to encourage creation of local language interfaces for Cloud services.

A recent index of risks associated with data centers ranked India and China poorly based largely on the presence of political risks from regulations and controls on investment and other aspects of data center installation.

Creation of a single window clearance process for data centers could go a long way in mitigating these perceived disadvantages.

**Special financial provisions** should be made available by the Indian Government for the private players who wish to build infrastructure for cloud computing.

**Cloud Infrastructure** - Private Cloud players should be allowed to procure raw infrastructure such as servers, firewalls etc at a subsidized rate for setting up the Cloud infrastructure.

**Loans** - Government should incentivize Banks to extend loans at concessional rates to entrepreneurs planning to set up Cloud services.

**Tax incentives** - CSPs should be granted exemption from paying regular taxes for a limited period of time from the time of setting up the Cloud operations.

**Land** - State governments should be directed to provide land at subsidized rates for setting up Cloud Datacenters.

**Smart Cities**: At the center of Internet-scale smart-city service delivery are domain-independent **service-delivery platform providers**, who present a new type of Platform as a Service (PaaS) offering that integrates IoT devices and infrastructures, processes data from a large amount of distributed data sources in real time, and lets applications employ both IoT and cloud resources on demand. The management of both IoT infrastructure and cloud resources is hidden from application providers. Platform providers must ensure the required provisioning of computing resources involved in service delivery. The platform also provides cloud services, including service metering, billing, and tenant management that will let stakeholders share resources and establish flexible business relationships.

Such a platform's emergence will directly influence traditional **domain-specific solution providers**. With a cloud-based platform, solution providers can leverage cloud resources to integrate IoT infrastructure and develop domain-specific applications, thus enabling virtualized vertical solutions, or *virtual verticals*. In virtual verticals, solution providers can reuse software

services on the cloud and scale up services without investing in the computing infrastructure. In addition, other than the traditional role of providing vertically integrated IoT solutions, solution providers can also provide IoT Infrastructure as a Service (IaaS) on the cloud to open IoT **device capabilities** to third-party application developers.

The platform will also benefit cloud **application providers** who specialize mainly in Web and cloud application development. The service-delivery platform lets these providers access IoT services to create novel applications for users. Application providers won't need domain-specific knowledge for managing IoT infrastructures because such infrastructures' capabilities are provided as services on the cloud, and the platform facilitates the important components for service delivery. Thus application providers can focus on application logics and enjoy on-demand use of both cloud and IoT resources.

**Q19. 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?**

**EBG Response:**

Each agency typically maintains its own data centers and server farms, resulting in hundreds of independent Government data centers. Reducing redundant infrastructure and services will lower energy consumption and improve data sharing among state and local governments.

Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS) vendors must be on an approved government shortlist in order to provide services to government agencies.

One of the most ambitious examples of how governments can take advantage of cloud computing is India's Unique Identification (UID) project. The UID aims to provide a positive change to the lives of the people at the bottom rung of the economic pyramid simply by providing a real time service for the verification of the identity of any Indian resident through biometrics or demographic information. The UID's advantage is that it's a generalized online service that is accessible by a wide variety of national, state, and local government authorized agencies as well as private businesses. The previous e-governance systems were limited in comparison, having been dependent on individual ministries and lacked standardization.

Currently, India's UID Authority has already collected the biometric and demographic information from over 200M people, and several government agencies are starting to use it for their systems. The future success of the UID may act as the herald of public cloud computing's success in the country, offering truly affordable, scalable, and sustainable solutions to an emerging market with acute public needs.

**Q20. 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?**

**EBG Response:**

Power: Electric supplies from the grids are erratic and backup solutions are expensive and additional infrastructure. Alternative Solar energy may be a solution.

Trained manpower: data centres require specialists to operate them efficiently. Merit based appointments with proper salary levels commensurate with the private sector need to be set for professional running of data centres. Security vetting of data centre manpower will be essential. Availability of affordable housing and amenities near data centers for personnel managing them (in order to attract high quality talent)

Big data handling: information sharing in India will not be equivalent to that of Europe with a population of 740million approx. With 1.3 billion people Indian statistics are bigger than most other countries. Government should be ready to upgrade and spend – within reasonable limits – on the latest big data technologies

Data sharing across borders will have to be regulated by new laws, if necessary, as currently water disputes, power sharing and distribution and a host of issues comprising migration and criminal activities across state borders face administrative problems.

**Q21. 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?**

**EBG 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.