Association of Unified Telecom Service Providers of India

AUSPI/12/2016/025 5th September, 2016

Advisor (QoS),
Telecom Regulatory Authority of India,
Mahanagar Doorsanchar Bhawan,
JawaharLal Nehru Marg,
New Delhi – 110002.

Subject: AUSPI's Response to the TRAI Consultation Paper on Cloud Computing

Dear Sir,

We are pleased to enclose AUSPI's response to the TRAI Consultation Paper on Cloud Computing for your consideration.

Thanking you,

Yours sincerely,

Ashok Sud
Secretary General
Mob: 9312941515

Encl: As above

Copy to :

1. **Shri R S Sharma, Chairman, TRAI**
2. **Shri Anil Kaushal, Member, TRAI**
3. **Shri Sudhir Gupta, Secretary, TRAI**

B-601, Gauri Sadan, 5, Hailey Road, New Delhi - 110 001
Tel. : 23358585, 23358989 Fax : 23327397
E-mail : auspi@auspi.in Web : www.auspi.in

AUSPI's Response to the TRAI's Consultation Paper on 'Cloud Computing'

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.

AUSPI's Response

Cloud computing is a technology for enabling service users to have always-on, anywhere, anytime availability of access when needed to share a pool of consumable computing resources that can be rapidly provisioned with minimal management efforts. We believe that large quantity of computing resources that is available as a cloud shall provide hosting environment that is immediate, flexible, scalable, secure and available when needed

Traditional IT set up requires enormously long period to set up whereas Cloud Computing Services (Paas, Laas, Saas etc) can be requisitioned immediately without delay. Traditional set up results in under /over provisioning whereas computing clouds provide hosting environment that is immediate, flexible, scalable, secure and available. Cloud Computing is simple for expansion of service due to elastic resource availability and economical as it depends on usage. It is possible to connect physical resources into virtual storage and virtual network in to cloud infrastructure and it is possible to tear down the virtual resources on demand. In addition, current cloud solutions also provide various applications.

Apart from the clauses suggested above, for ensuring smooth migration of the customer's setup, following provisions are needed for live migration to cloud and for migration from one cloud service provider to another:

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

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

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

AUSPI's Response

Cloud offers a platform for hosted deployment, faster deployment and availability of services that are affordable as they exploit the benefit of economies of scale. Cloud service providers optimize the pricing by building an optimized pool of computing resources along with an automation layer. This approach ensures maximum utilization of available resources enabling faster RoI. CSPs pass on these benefits to customers in terms of pricing etc. CSPs scale business, decrease time to market and enhance collaboration with the cloud ultimately leading to costs advantages. The key issue for cloud adoption is therefore, price flexibility, cost efficiencies of the users, easy infrastructure and application scalability, speedier deployment of infrastructure etc.

There have been many studies which concluded that adoption of cloud computing would bring better economies of scale vis a vis in house IT setup and benefit through reduced costs of IT Infrastructure and Power and with increased focus on core business functions of enterprises. However, the cost saving is dependent on the scale of data centre and time taken to shift to cloud.

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?*

AUSPI's Response

Several factors influence business enterprise decisions, depending on which type of solution is preferred, i.e. capital and expense budgets, the degree of in-house technical expertise etc.

Some of the important parameters for selection of type of cloud service depend on the following:

- Guaranteed performance at reasonable cost
- Performance flexibility to ensure smooth delivery
- Availability of 24x7x365 power supply
- Reliability and maintainability
- Security – physical and data
- Storage and back up
- SLAs, Reliability
- Ease of billing and billing verification
- House skills
- Compliance and control requirement and certification

We feel that while business of all size benefit from the efficiencies of cloud services, cost saving due to impactful dimension of cloud service actually benefit the SMEs.

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?

&

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

AUSPI's Response

Many issues need to be addressed when migration is being considered from one cloud to another. We feel that each technology evolving for cloud, a standard format is desirable though may not be immediately possible. We, therefore, suggest the following points amongst others:

- An agreement may be provided for customer's data in open format.
- In case of migration outside India, Government need to be kept informed.
- Signing of appropriate Non-Disclosure Agreements and compliance of the Government's Remote Access provisions
- Before initiation of the migration of services, establishment and migration of services to disaster recovery system should be mandated.

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?

AUSPI's Response

Moving application/data in and out of the cloud can be due to customers or CSPs requirement. In order to ensure that the customer is able to have control over his data while moving in and out of the cloud, we suggest the following:

- Approval of the data owner, before initiation of the migration process.

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

- Adoption of ISO/IEC code of practice for protection of personally identifiable information in public cloud.

We feel that, over all, light touch regulation is required, but TRAI may prescribe internationally adopted, accepted and followed codes of practices to cover cloud computing issues such as data ownership, information security, etc.

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?*

AUSPI's Response

It is imperative to ensure that the CSPs do not introduce direct / indirect barriers for customer applications to interoperate. The modern entrepreneurs must retain their freedom and ability to innovate and create differentiation from competitors to ensure successful business operations for which interoperability of cloud services is a must. CSPs may be encouraged for self-certifications for their openness in the market by using internationally accepted open network and support traditional movement of data.

The regulatory framework and standards for ensuring interoperability of cloud services should be prescribed to adhere global interoperability standards instead of having proprietary, India specific standards.

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.*

AUSPI's Response

QoS is perceived by user basis on various key parameters like

- Performance
- Availability
- Security and resilience
- Reliability
- Metering and billing accuracy
- Support in compliance of regulations
- Response time and customer support.

Since clouds are measured on different dynamic and static parameters, the cloud services should be monitored and managed at multiple layers of network applications.

QoS is a matter of contractual negotiation between the parties. Any dispute needs to be settled through the arrangements in the contract. Regulatory intervention on QoS for cloud computing is not necessary.

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?*

AUSPI's Response

The matter of billing and metering revaluation by customers of cloud services is extremely important and in this connection we suggest the following:-

- Cloud Service providers should maintain a detailed log of online actions executed for the customer.
- These logs should capture customer ID, action taken, timestamp and source device logical address so that complete audit trail and record is available.
- These logs should be stored for six months for record keeping and dispute resolution.
- Customer should have easy access to this data and in case of any dispute both parties can review these logs together and come to a mutual consensus to resolve the dispute.
- Customers should be provisioned instantaneous/periodic feedback about their usage.
- Provisioning of a trusted, may be government approved, third party tools / mechanisms for measuring the consumption of data at the user's end, similar to the apps that are available for measuring data consumption in a user's handset.
- CSPs be subjected to mandatory billing and metering audit through government / regulatory body accredited auditors similar to the practice being followed for the telecom services.
- Establishment of an appellate mechanism for billing dispute resolution.

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

AUSPI's Response

a. It should be mandated for the CSPs to establish a customer support team and advocate its accessibility through requisite means for both B2B abd B2C customers.
b. A CSP provisioning paid services for the B2C segment should be mandated to provision customer support similar to what the TSPs are mandated to provision.
c. Requisitioning of level of customer support service, above a set of basic services, should be left to mutual agreement between the B2B customer and the CSP.
d. An external agency or a central mechanism like an Appellate mechanism for resolution of issues of cloud services should also be established.

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.***

AUSPI's Response

From the regulatory perspective, a self-certified regime needs to be established for self-accreditation. Some important provisions amongst others required for ensuring that the cloud services being offered by the cloud service provider is secure are as follows.

a. Mandatory hosting of services for a user base greater than one million.
b. CSPs to share their security governance processes and capabilities.
c. To regularly update and publish their information security processes and procedures and Governance mandatorily.
d. Mandatory provisioning of information about any breach of security in any domain.
e. Compliance to a process driven Change Management before implementation of any change in the cloud environment.
f. CSPs to ensure that their systems are updated with the latest OS patches and security software updates.

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

AUSPI's Response

It is necessary that the data user should be assured of complete deletion of all his data (and any traces thereof) once the user decides to terminate the services of the CSP and exits out of his Data Center. The exit or termination clause is transparently decided upfront during the process of requisitioning of the services itself and is legalized in their SLA and contract. Following termination or exit provisions may be defined for ensuring security of data or information over cloud:

a. On execution of the exit / migration clause of the agreement, first and foremost the user's data should be handover to him in an open readable format which is acceptable for use.
b. Post due verification and approval from the customer, the process for deletion of the customer's data should be initiated by the CSP.
c. It is the responsibility of the CSP to permanently delete all the customer related data, including the backups.
d. The CSP should be obligated to inform the customer about the completion of the mandated period of CSPs jurisdictional regulated retention and subsequently about the complete deletion of the retained data.

e. The CSP should be mandatorily obligated to ensure that the VM related data of the customer's VMs, collected during routine VM introspections, is not shared with any other customer with or without any monetary consideration.
f. The customer too should be obligated not to disclose any of the technical expertise / operational models / any other operational details of the CSP's cloud services setup to any of its competition.
g. CSP should be mandated to ensure that the data cannot be forensically recovered and ensure that all the documentation like policies, procedures, asset registers, configuration documents etc kept up to date and handed over to the customer during the exit management process.

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

AUSPI's Response

As per the Cloud Security Alliance's (CSA) guide, security ownership in Cloud varies as per the Cloud Service Deployment models as follows:

1. **Cloud Service Provider.**
   a) Adherence to security processes and procedures as listed in response to question no 10 above.
   b) Obtaining and maintaining certification of the services and security levels offered by the CSP.
   c) Ensuring data integrity and confidentiality.
   d) Ensuring clean deletion of data from older storage systems once they are being removed / replaced.
   e) Access to the data Centers through proper verification and by authorized persons only.
   f) Conduct of due police verification of each and every individual employed in the data center.
   g) Adherence to the security instructions, regulations and laws of the land / any agreements that bind the CSP to the laws of a distant land.
   h) Ensuring compliance of SLAs agreed with the user.
   i) Ensuring compliance of all CSPs obligations by the third party outsourcing partner.

2. **Application Provider / B2B user.**
   a) Enactment of stringent SLAs with the CSP.
   b) Data preservation strategy and guidelines.
   c) Ensuring VAPT of the proprietary application being hosted in the cloud infrastructure.
   d) Building redundancies into its services.
   e) Ensuring confidentiality of information.
   f) Ensure no sharing of user's information to maintain his privacy.

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

3. **User.**
   a) The maturity, effectiveness and completeness of the risk adjusted security controls implemented by an organization, at different levels viz Physical Security, Network Security, System Security and Application Security including Information Security, determine the level of security that an organization is willing to accept.
   b) Subscription to the services for a disaster recovery at a different physical location and may be a different cloud service provider as well.
   c) The level of data resilience and redundancy opted for storage of data is solely dependent on type of service opted for.
   d) The user is completely responsible for the security and protection of data in the user's device.
   e) It is the users' responsibility to ensure proper cyber hygiene for the user's devices and equipment.

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?

AUSPI's Response

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

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

Q 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?

&

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?

AUSPI's Response

There is an urgent need for international cooperation in the fight against transnational crime and terrorism. In the cyber space, the need for such international level agreements gets further accentuated due to the internet's inherent ability to provide seamless access to distant locations sans any boundaries. India should have maximum possible number of "Mutual Legal Assistance" agreements and should encourage local hosting of servers and applications.

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

AUSPI's Response

With global footprint of CSPs, it is best to enact and strengthen other laws and agreement for bringing violations of CSPs in to the scope of law.

It is submitted that a light touch regulatory regime that facilitates growth of CSPs while addressing national security concerns is most desirable. The following Acts also govern Cloud Computing Services

i. Income Tax Act, 1961.
ii. Consumer Protection Act, 1986.
iii. Payment and Settlement Systems Act, 2007.
iv. Indian Copyright Act, 1957.
v. Central Excise Act, 1944.
vi. Prevention of Money Laundering Act, 2002.
vii. Information Technology Act, 2000.
viii. Foreign Exchange Management Act, 1999.
ix. Customs Act, 1962.

Cloud computing should not be subjected to the Indian Telegraph Act 1885. CSP should be asked to register themselves as Other Service Providers (OSPs) with the government of India.

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.

&

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?*

AUSPI's Response

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

1. **Development and Availability of Local content.**Government's 'Make in India' initiative shall give an impetus to easy availability of basic tools like mobile phones, cameras, scanner, video recorders etc. for content creation and include measures like removing any trade barriers, taxes or levies that limit the development, production and importation of these devices.
2. **Availability of Internet Infrastructure.**

    a. **Exemption of 'Right of Way' (ROW) charges for laying optical fibre:** Exempting ROW for rolling out the fibre network to provide high speed broadband services shall entice global content owners to move the content in the country for better accessibility & at affordable cost.
    b. **In-building Solutions:** Free and neutral access to all Multitenant Campuses, Buildings, Apartments and other buildings should be mandated.
    c. **Promoting Local Hosting of Content, encourage local hositng.** Local hosting of content ensures better user experience of services utilization over the internet and utilisation of local man power.
3. **Encouraging business and private organizations utilize cloud services.**

4. Coupled to solving the above mentioned impediments, enactment of laws that make the businesses feel secure about their data and privacy would go a long way in encouraging them for adoption of cloud based services.

5. Embracing Cloud services for government projects such as smart cities and e-governance.

6. Increase in carbon credits can be leveraged to incentivize SME and enterprise segments

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?

AUSPI's Response

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

a) Government services are provisioned for and are requisitioned by all the citizens of a country and therefore, require:

- ⇨ Better and optimised administration of the setup.
- ⇨ Better database optimization.
- ⇨ Better utilization of the resources as idle resources can be deployed for supporting services that might be facing peak loading.

b) Economies of scale, multi-tenant setup, high level of security, etc of cloud characteristics can be exploited for multiple applications of the government hosted in single cloud setup.

c) The provisioning of government services through the cloud would be akin to essential services and hence, should be from an exclusive, open standards based, cloud setup hosting only the governmental services.

d) The cloud setup established for provisioning government services can be hosted in the government data centers or can be hired from private operators. Even if the setup is hired from private parties, hosting of only government services should be mandated, within that setup.

e) The setup should be mandated to be highly robust by provisioning multiple levels of redundancies, high grade resilience and near real-time disaster recovery capabilities.

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?

AUSPI's Response

i. Data Center being a specialised establishment, it is imperative that the primary selection criteria of the vendor for building it should be more on technological expertise and operational competence rather than commercial considerations.

ii. Tenders for IT and Non IT requirements should be two separate tenders instead of single tender.

iii. SDCs should be viewed as an essential infrastructure for the state and should be housed in a separate specially built building rather than retrofitting an existing office building & it should be designed with due modularity and expansion capability.

iv. Long term maintenance and operation of services with skilled technicians.

v. The State Government, as part of Skill Development programme, should appoint the basic man power requirement of the data centre.

****