ORACLE

Feedback on "Consultation Paper on Cloud Computing" – TRAI

Oracle India Private Limited

Question 1. What are the paradigms of cost benefit analysis especially in terms of:

a) Accelerating the design and roll out of services

The following are the various aspects of the design that has to be considered for successful rollout of any ICT project including that on Cloud.

- Scalability
- Availability
- Performance
- Manageability and Security

All the above aspects have to be considered across various layers of infrastructure like Web / Application Layer, Process Layer, Information Layer, Compute & Storage Layer, Network Layer for any new initiative to succeed. Once such a complex environment is setup, in this ever-changing world of technology this has to be upgraded on a timely basis to avoid exposing the setup to security threats and obsoleteness. Hence such environments were in constant sustenance mode. These sustenance services in a traditional approach always consumed majority of the IT budgets just to 'keep the lights on'.

Studies done of economics of "keeping the lights on", shows that roughly 70% of the budget is spent on sustaining and running existing capability while only 30% is spent on providing new capabilities to the business[1]. Moving such services to cloud will lead to significant cost saving and better utilization of IT budgets.

[1] Gartner – "Making the Difference: The 2008 CIO Agenda" (Jan 2008).

Additionally, Cloud accelerates deployment life cycle by reducing infrastructure lead times, improves time to introduce new services/products through automation and promotes innovation. It also makes management and operations optimized which offers significant cost savings while improving the overall efficiency as well.

b) Promotion of social networking, participative governance and e-commerce.

In a vibrant government, citizen participates in the decision making process. With India heading towards becoming one of the highest Internet Penetration in the world, Social Media, Networking has become the most transformative means of engaging the citizens. On a larger canvas this called the 'Digital Disruption'. It is very much essential that government adopts this 'Digital' wave for maximum impact with citizen. The same has been answered in details under "Steps that can be taken by the government" (*Question 18*)

For applications (where PI data is not stored) and for promotion of social networking, Public cloud must be leveraged as new technology would be tested and new services would first be made available on public cloud platform.

c) Expansion of new services.

Traditional expansion of Services involves Procurement and Deployment of environments for Development, Testing, Pilot and Production Environments. All these activities create inherent delays, escalation of costs and in most cases. Traditionally, it is noted that while moving to production environment, rest of the environments likes Development, Testing were discarded causing loss to the exchequer. In cloud environments the commercial constructs and ability to provision environments for a given size and time share basis helps in improving the overall total cost of ownership. Additionally, in most of these cases the Test environments are allowed to be fork lifted into production environments saving significant costs. This feature is supported from an On Premise to 'Cloud' setups too. Pivoting on premise workloads to cloud helps to improve agility , elasticity, helps to rapidly provision apps using infrastructure cloning, results in significant cost savings by about 40-60%. This also creates the innovation of tools that can further optimize the migration exercise and reduce costs.

Latest technologies are available that can help 'migrate to cloud' quickly and easily can solve the following:

- Lift and shift VMWare and KVM Workloads to the Cloud without any changes
- Automate "V2C" migration of fully functioning applications
- Nested virtualization
- Software defined networking, storage overlay, automatic capture of applications

d) Any other items or technologies. Please support your views with relevant data.

Some of the benefits of moving to the cloud that you can list are –

1) Access to the latest software versions with your subscription. No need to run expensive upgrades.

2) High degree of availability – Cloud providers are extremely reliable in providing their services, with many maintaining 99.9% up time. The services are always up and available.

3) Improved access – Service and applications are available to employees from anywhere in the world. Employees can access services from mobile devices.

4) Collaboration – Cloud applications can improve collaboration between geographically spread out teams as it easy to share information that sits on the cloud.

5) Environmental impact – With fewer datacenters worldwide and with more efficient operations, cloud allows customers to bring down the size of their Data Center's along with space, power.

6) Business Agility – Need to response quickly to changing business requirements and prioritization

7) Time to Market– Need to maintain, on-time, on-budget delivery of application releases

8) Cost Optimization– Need to Reduce infrastructure CapEx, data center OpEx,and IT staff resources

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

ORACLE

Clouds' these days, are built for enterprise grade real world scenarios. The providers of cloud services are catering to enterprise markets of Governments and Corporate in highly Mission Critical mode round the clock. Successfully catering to these requirements has ensured Standardization and homogenization of data center technologies.

Standardization and Homogenization requires significant investments running into millions of dollars for Research, Development and Sustenance. Thankfully, most of the cloud service providers work on 'Shared' architectures with logical/ physical separations creating economies of scale. Thus, shared architectures (basis of cloud services) lead to significant cost reduction.

Besides Technology, Architectural innovations, the cloud service providers offer various commercial constructs that helps in reducing the total cost of ownership. It is to be noted that by design the basic tenet of a 'Cloud' commercial offering is to allow consumers to move their Capital Expenditures (CAPEX) to Operational Expenditures (OPEX).

Question 3. What parameters do the business enterprises focus on while selecting type of cloud service deployment model? How does a decision on such parameters differ for large business setups and SMEs?.

No single strategy fits all .Initially; it was observed that customers were adopting cloud more out of cost benefits but the trend of journey to cloud is more due to Agility, Increase in innovation and Digital Experience to Customers/ Citizens etc. Cloud adoption by businesses depends on perspectives like Business Vision, IT Maturity, People, Processes, Security and Budget considerations. A thorough evaluation needs to be done to select the correct deployment model for cloud. Currently offered deployment models listed below

- Private clouds (hosted for a single organization)
- Public clouds at Service Provider (remotely over the Internet)
- Public cloud at customer's Data Center (behind their Firewall)
- Hybrid clouds (combination of on-premise and on-cloud)
- Community clouds
- Federated clouds
- Multi-clouds

Primarily for large enterprises, the following can be key considerations :

a) A combination of Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) platform/services made available from a domain.

b) End-to-end Security

c) The cloud platform should support hybrid (on-premise & on-cloud) with integration.

d) Maximum Availability Architecture deployment at cloud to protect against data, server, site failure.

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

An enterprise grade 'Cloud Service' provider will ensure customers against vendor lock in using the best of breed architecture and standards. Additionally, provide migration tools and standard practices that help customers migrate instances and data from one cloud platform to another. Pivoting on premise workloads to cloud helps to improve agility , elasticity, helps to rapidly provision apps using infrastructure cloning, results in significant cost savings by about 40-60%. This also creates the innovation of tools that can further optimize the migration exercise. New tools, processes and methodologies have been developed to

migrate heterogeneous workloads, set standards and use multiple cloud /on premise touchpoints as source and targets.

Question 5. What regulatory provisions may be mandated so that a customer is able to have control over his data while moving it in and out of the cloud?

Some of the regulatory provisions that may be mandated are policies related to

- Control : Security mechanisms to control who can access data and under which conditions
- Auditing : Ability to audit resources to maintain their security configurations
- Visibility : Logs providing visibility into accounts and resources
- Assurance : Ability to independently verify how data is being stored, accessed, and protected against unauthorized access and modification
- Security : Services that are designed, coded, tested, deployed, and managed securely
- Out-of-the-box integration with existing technologies: Seamless integration with existing solutions such as identity and access management

However, it should be flexible for based on data, nature of application and specific requirement of business enterprise, government & service provider. The effectiveness of this policy should be in a completely automated enforcement and monitoring. For example, OEM's security philosophy is built around the following approaches:

Preventive strategy based on defense-in-depth. It is believed that there is a need to drive down the perimeter and add security controls closer to the data. In addition to having a defense-in-depth preventive strategy and development of strong and effective processes for breach detection, incident response, and effective remediation is continued.

Now-a-days security and trust models are being re-defined for cloud computing. For example, traditional administrator model based on the powerful, full privileged administrator concept are being replaced with a model that places more power with the consumer. The service provider should manage only the infrastructure objects, and doesn't have any channels to access customer data.

Mature service providers employs some of the world's foremost security experts in information, database, application, infrastructure, and network security. They offers a comprehensive IaaS and Platform as a Service (PaaS) portfolio that share a common set of security capabilities such as identity and access management. It includes services such as Compute, Storage, Networking, Database, Java, Process, Mobile, Data Management, and Business Analytics, which is used by organizations worldwide, from large enterprises and the most demanding governments to small enterprises.

Question 6. What regulatory framework and standards should be put in place for ensuring interoperability of cloud services at various levels of implementation viz. abstraction, programming and orchestration layer?

Interoperability and portability standards for 'Cloud Services' are in phase of evolution. To promote a balance between healthy innovation and growth at the same time. Cloud service providers at the least, need to subscribe to standards like Open Virtualization Format, Open Cloud Computing Interface, Cloud Data Management Interface etc.,

With respect to Implementation, Pivoting on premise workloads to cloud helps to improve agility , elasticity, helps to rapidly provision apps using infrastructure cloning, results in

significant cost savings. New tools, processes and methodologies have been developed to migrate heterogeneous workloads, set standards and use multiple cloud /on premise touchpoints as source and targets. There are many tools and solutions in the industry that helps to provide a seamless lift and shift experience driving standardization.

Question 7. What shall be the QoS parameters based on which the performance of different cloud service providers could be measured for different service models? The parameters essential and desirable and their respective benchmarks may be suggested.

Some of the key QoS parameters that are used to measure the performance of cloud service are:

- Elasticity
- Reliability
- Availability
- Durability

Cloud Providers also use a variety of software tools to monitor above parameters of Customer's production services environment and the operation of infrastructure and network components to ensure that there is no service degradation. Again, the focus should be on end to end automation.

Question 8. What provisions are required in order to facilitate billing and metering re-verification by the client of Cloud services? In case of any dispute, how is it proposed to be addressed/ resolved?

Detailed billing metrics are available to customers from the cloud providers. Customers have the flexibility to procure services on demand (Pay as you go) or on a pre-paid model (Reserved). The services consumption is usually charged on a per hour basis on the first model and is fixed in the latter and the consumption per hour is recorded in the customer's usage and billing. This fine grained billing view gives the customer to control their billing and service usage. Should there be issues with the bills generated; customers can reach out to the service provider who would also maintain detailed billing metrics. All these are to be provided thorough standard Service Level Agreements for maximum transparency of provisions.

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

Such incidents are typically handled through a customer support channel, which offers support in terms through emails, calls and some on-site consulting and advanced support on need basis. Customers will usually be able to subscribe various support models ranging from basic, to premium to enterprise- each offering various levels of support at different price points.

Question 10. Enumerate in detail with justification, the provisions that need to be put in place to ensure that the cloud services being offered are secure.

Cloud infrastructure and platform services operate under a shared responsibility model, where the vendor is responsible for the security of the underlying cloud infrastructure, and consumers need to decide and choose the security levels based on various solutions that are offered by the vendors. This shared responsibility model is key to ensure that the ecosystem is fully secure.
The same has been answered in details under security provisions questions (*Question 12*)

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

In general, customers can terminate their contracts based on the terms in their contracts. For instance, Pay as you go customers will be able to terminate at any time the services. Usually for a period of up to 60 days after the termination or expiration of production services, service providers will make available customer production data for the purpose of retrieval.

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

Customers can be privy of the following aspects to ensure that they have control of their data and instances during migration

- Data Privacy and Data Protection
- Security of data at rest and in transit
- Secure channels for data transfer
- Disclosure and Cross-border movement of data

It is recommended that all Cloud Applications housed in the Government Cloud on the lines of The Federal Risk and Authorization Management Program (FedRAMP). FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. The security assessment process uses a standardized set of requirements in accordance with FISMA using a baseline set of NIST 800-53 controls to grant security authorizations.

We are also working with federal customers willing to conduct Assessment & Authorizations (A&A) and sponsor Oracle for a FedRAMP Agency ATO on a feasibility basis. The Sponsoring agency can initiate the FedRAMP process and follow the FedRAMP approved security assessment process as the path to grant an Agency ATO. FedRAMP Agency Authority to Operate is an efficient method to obtain an ATO compliant to the FedRAMP controls and mandate

Further, live migration of virtualized application to cloud ‘as-is’ can be achieved using latest technology offerings. Such cloud services enable migrate on-premise VMs to run natively on cloud without need for third party hypervisors. It clones in minutes using blueprinting technology. The VMs will continue to work as if deployed within your data center.

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

Cloud infrastructure and platform services operate under a shared responsibility model, where the vendor is responsible for the security of the underlying cloud infrastructure, and consumers need to decide and choose the security levels based on various solutions that are offered by the vendors. This shared responsibility model is the key to ensure that the ecosystem is fully secure and should be mandated.

The roles and responsibilities of various stake holders are usually covered in the policy and service delivery documentation. For instance, cloud service providers are responsible for the

security of everything at the infrastructure and hypervisor level while customers are responsible for securing the data and workloads that run on top of them.

Further, the policy should be flexible enough to allow the management of cloud platform from anywhere outside the country, so that 24 by 7 management operations can be achieved.

Question 14. The law of the user's country may restrict cross-border transfer/disclosure of certain information. How can the client be protected in case the Cloud service provider moves data from one jurisdiction to another and a violation takes place? What disclosure guidelines need to be prescribed to avoid such incidents?

To implement these processes requires additional resources, investments to monitor/ control movement of data. Hence a fine balance has to be maintained between having this feature 'ON' and 'ON DEMAND'. This will allow the scale of economy that is expected out of 'Cloud Service'. Having stated that, the service provider should support the ability to add additional monitoring, reporting of movement of data on a 'Demand basis' to make this effective. A key feature of this ability must be the ability to configure, encrypt, label data right onto the database layer by the subscriber on a self-service mode.

In the current scenario, there has been an acknowledgement of these concerns by the IT industry in general. This is reflective of the increase in focus on Hybrid Clouds and Public Cloud at Customer's Data Center. Cloud at Customer's Data-center is an interesting model that has emerged where in the data security concerns are addressed by hosting data within the customer data centers/on-premise. This shrink-wraps the cloud into a machine residing in the customer premises without compromising any commercial benefits of public cloud offerings. It is highly recommended to adopt innovations like this at early stages to foster growth and increase cloud adoption.

Question 15. What polices, systems and processes are required to be defined for information governance framework in Cloud, from lawful interception point of view and particularly if it is hosted in a different country?

Comprehensive data security policy must be setup ensuring that the process is not just a mere manual observation, sampling and reporting but a completely automated, self service policy that addresses Data at Rest, in Memory, Data in motion with perimeter security. These policies should be able to detect, alert and in extreme cases prevent the application from functioning on violations.

A pointed case within our company is stated here.

Customer data whether it is held on our hardware assets or on the personal hardware assets of our employees and contingent workers follows global standards of security. When Oracle's Global Information Security (GIS) organization is informed of such as incidents mentioned above and, depending on the nature of the activity, it defines escalation paths and response teams to address those incidents. GIS will work with Customer, and the appropriate technical teams, and law enforcement where necessary to respond to the incident. The goal of the incident response will be to restore the confidentiality, integrity, and availability of Customer's environment, and to establish root causes and remediation steps. Operations staff has documented procedures for addressing incidents where handling of data may have been unauthorized, including prompt and reasonable reporting, escalation procedures, and chain of custody practices. This entire process is automated for effectiveness.

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

Please comment with justification

.

- No Comments

Question 17. What should be the protocol for cloud service providers to submit to the territorial jurisdiction of India for the purpose of lawful access of information? What should be the effective guidelines for and actions against those CSPs that are identified to be in possession of information related to the commission of a breach of National security of India?

- No Comments

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

(a) promoting cloud computing in e-governance projects.
(b) promoting establishment of data centres in India.
(c) encouraging business and private organizations utilize cloud services
(d) to boost Digital India and Smart Cities incentive using cloud.

Government must consider Public Cloud platform, for promoting digital strategies like smart cities etc. Depending on type of data (if the data does not include Personal Information), then Public Cloud, irrespective of the country of data residency, must be leveraged.
In case, the type of data include PI data, then Public cloud services should be made available from within customer's data center.

Further, the management of cloud platform should be allowed from anywhere outside the country, so that 24 by 7 management operations can be achieved.

For instance, NIC can consider an investment to offer such services by procuring resources and providing power, space, cooling, etc for the resources.

The process of recruitment of Cloud Service Provider (CSP) should be a dynamic process, allowing addition/deletion of CSPs depending on if they have a Data Center in India.

A summary of various successful implementations worldwide is as below

1.) Establish City Wide Nervous System
2.) Maximize Reuse of Infrastructure
3.) Provide a Sentient City Infrastructure
4.) Integration platform with External Agencies

Typical activities involved in achieving success to boost the digital revolution is as below

Engage Citizens: Deliver great citizen experience throughout the citizen journey, and across all interaction channels with government agencies. Socially, enable all departments, empower mobile access anywhere, and apply learned insights from actionable data, all with the speed and agility of the Cloud. E.g. The Oracle Customer/Citizen Experience Cloud helps government agencies to transform citizen relationships into pro-governance and active relationship

Get Social **:** Our vision is to socially enable the government agencies to provide a better understanding and engagement with customers and stronger collaboration and efficiencies within the workforce. Every organization should have the tools to integrate social seamlessly across every mission-critical department — to listen, engage, collaborate, manage and maximize social media for business efficiencies that will lead to an enhanced customer experience

Empower businesses: Streamline process of Energy Utilization, Registration, Permits, Commercial taxes and Check post management, Environmental Clearances using digital solutions of Internet of Things, Big Data, Social Listening, and Mobility etc. This has to be seamlessly integrated with government agencies to ensure maximum productivity of businesses with transparent delivery of government services.

Question 19. Should there be a dedicated cloud for government applications? To what extent should it support a multi-tenant environment and what should be the rules regulating such an environment?

A parlance can be seen with many transformative services that were introduced in the past two decades in India. Similar questions are being raised on 'Cloud Services' too. For example when 'Internet Service' was initially introduced in Government and Citizen services, it was restricted for dedicated environments and applications but over a period of time due to large scale of adoptions and advantages we see majority of Devices, Servers, Systems, Applications being connected to the Internet. Off Course, security, regulations etc have also evolved with it. Similar trends are being observed in 'Cloud Service' and 'Cloud Offering'

Multi tenancy may be understood as ability to host multiple departmental applications (for a government customer) on a shared platform creating a Common Operating Model, Elasticity, and Security, with Individualized Metering, Billing and Monitoring. Besides the typical SLA requirements, it is expected that the multi tenant model should support isolations from Application to Storage level including support for customizations and upgrades as mandatory

Question 20. What infrastructure challenges does India face towards development and deployment of state data centres in India? What should be the protocol for information sharing between states and between state and central?

Current SDC's in India are in varying degree of maturity based on the individual state's vision and priorities. They have also evolved over a period of time with every state being different on the below mentioned parameters

- Standards
- Security Policies
- Availability Requirements
- Manageability Process, etc.

These inconsistencies impact cross departmental data sharing and process standardization leading to silos of information. Ultimately, impacting quality of critical government initiatives like 'Paperless Office', 'Single Window Clearing' etc.

State Data Center can standardize at offering Public Cloud services, both IaaS and PaaS from within their data-center by investing in cloud solutions which offers Infrastructure as a Service and Platform as a Service for Database, Java, Integration, etc.

ORACLE

On Data Sharing Challenges: Challenges between state and central agencies has been there even without the advent of Cloud. In the past, India has achieved a great degree of cohesion between multiple agencies in many cases like for e.g. Right to Information Act (RTI) in Government; Know your Customer (KYC), Credit Scores (CIBIL) etc. It is preferred that a common Data Governance Policy be created on similar lines for effective Data Sharing between State and Central agencies.

Question 21. What tax subsidies should be proposed to incentivize 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?

Initiatives for promotion of Cloud Services in India can include :

- Cloud Service Providers (CSPs) and/or National Informatics Center (NIC) can consider making an initial investment to offer Cloud Services to a Government customer from within their Data-Centers. This can be done, for instance,
    - By procuring resources and providing power, space, cooling, etc for the resources.
    - By offering Out-of-box DevOps capability, for application development.
    - By setting up a Center of Excellence and/or lab-setup, where they can incubate & test different cloud service, like Internet of Things, Mobility, Social, Artificial Intelligence / Machine Learning, ChatBot, etc.
- Adoption of latest innovations offered service providers in Public Cloud, by deploying non-confidential applications there and reducing the learning-curve.