AWS Response to TRAI Cloud Computing Consultation Paper - Issues for consultation

Table of Contents

25 July 2016

To: Shri A. Robert J. Ravi
Advisor (QoS) TRAI
advqos@trai.gov.in
+91-11-2323-0404

Dear Sir,

Consultation Paper on Cloud Computing

Amazon Web Services (AWS) thanks the Telecommunications Regulatory Authority of India (TRAI) for the opportunity to comment on the Consultation Paper on Cloud Computing. We at AWS believe that public private consultations are an important way for industry to contribute to India's digital future. Industry consultations such as this one are important in ensuring that all stakeholders are engaged and involved in the process.

In building Digital India, we believe it to be good for the government to ensure clarity for all service providers, and as such, we commend TRAI on seeking to establish clarity through a transparent and trusted business environment for India's networked industries and cloud products and services.

Amazon has an extensive track record of investing in India. In 2016, Amazon CEO Jeff Bezos was honoured by the US-India Business Council (USIBC) with a Global Leadership Award, presented by Prime Minister Narendra Modi.[1] We have also committed investing more than USD3 billion recently in India, boosting Amazon's total investment to over USD5 billion[2], and on 28 June Amazon Internet Services Private Limited announced the launch of an AWS datacentre infrastructure region in India[3]. We therefore look forward to continuing to partner with you in building India's cloud computing future.

We welcome further engagement and discussions between TRAI and AWS on this matter. Should you require any additional information with regard to the contents of this response, please do not hesitate to contact me.

Yours sincerely,
Roger Somerville
Head of Public Policy, APAC
Amazon Web Services

[1] The Indian Express, 8 Jun 2016, PM Modi Presents USIBC Global Leadership Awards To Dilip Shangvhi, Jeff Bezos http://indianexpress.com/videos/news-video/narendra-modi-presents-usibc-global-leadership-awards-to-dilip-shangvhi-jeff-bezos-visit-us-2840766/

[2] The Hindu, 8 Jun 2016, Amazon to increase India investment to $5b http://www.thehindu.com/business/Industry/modi-in-us-amazon-to-increase-india-investment-to-5-billion/article8706252.ece

[3] https://aws.amazon.com/blogs/aws/now-open-aws-asia-pacific-mumbai-region/

Context and general comments

While we commend the TRAI on initiating this consultation, we also believe it to be worth setting some context. Soliciting input from the private sector to inform the regulatory and policy structures under consideration is sensible and, when handled constructively and in a well-coordinated approach, stands to be widely beneficial. Particularly when undertaken while keeping the government's overall objectives in mind. As such we suggest some overarching considerations that have guided our overall submission:

Clarity and Predictability
For the private sector to be able to make large-scale investments confidently, there needs to be clarity in the rule-setting environment and predictability in market development. It is this that enables business to make forward-looking investment. In this sense, TRAI's involvement as the oversight agency for the telecommunications and networking industries is understandable. We note also that the Department of Electronics and Information Technology (DeitY) has been taking an active role in setting policy agendas for many aspects of cloud computing and we hope the two agencies will take a coordinated approach to developing the cloud computing market in India and providing clear signals to the market on how the government would like to see the market develop.

Developing the Cloud market
Cloud computing is still at a relatively early stage of development with the potential therefore for extremely rapid growth. Nurturing, enabling and accelerating this growth will be good not only for India's ICT industry, but as numerous studies are beginning to demonstrate, it is good for national economic growth, business agility, and wider social development, including through promoting greater inclusiveness and government-citizen interactions. Frameworks set up to enable and promote broad-based development and growth should therefore be championed, and it is in this context and this spirit that we have provided our detailed responses to the consultation paper.

Regulation
Given the relatively early stage of cloud computing development we strongly caution against taking an overtly regulated approach to structuring the cloud computing industry in India. At this stage of the sector's development in India, we believe that a heavy-handed regulatory approach will likely inhibit growth. And while cloud is still at a relatively early stage in its growth, it is worth bearing in mind that much work has been done over the last decade in various industry standards bodies, and by the industry as well in establishing best practices. This is not to say that there is no place for regulation. In some areas, such as ensuring network equipment is safe, establishing data privacy frameworks or providing for consumer protection there may be cause for limited regulation. But we would encourage the Indian government and TRAI to look where possible to industry best practices, and we have made mention of this and provided examples in our specific responses.

Procurement
A related area to be considered is procurement of cloud services. Buying cloud services is unlike most traditional technology purchases. Customers are accustomed to buying IT infrastructure using procurement rules designed for traditional purchases such as data center hardware or software; however, such traditional purchasing approaches include procurement practices and contract terms that may inhibit adopting the scalability, lower costs and innovative nature of cloud technology. The industry would like to see an environment that allows for a fast and flexible acquisition process without onerous terms and conditions that enables organizations to extract the full scale and flexibility of the cloud.

Innovation

We would also like to emphasize the potential for local innovation to become squeezed in the event of over regulation. One of the biggest beneficiaries of cloud computing is the Small and Medium Enterprise (SME) market, as they are suddenly able to access enterprise grade ICT tools affordably and effectively. Utilizing cloud computing, SMEs are able to scale rapidly and, in many cases, are born as multinational export operations. At the vanguard of this in many markets is the e-commerce sector. Overtly regulating cloud computing tends to disproportionately impact SMEs as their costs, including for licensing, for compliance, and related issues, go up rendering the cost benefit analysis unattractive. India's e-commerce market is growing vibrantly and the innovation in the marketplace is rich, varied, and startling.

India as a Cloud leader

India stands to be an enormous market in cloud computing and to be an enormous global presence in the developments coming forth from the cloud computing sector. In the process of building Digital India, we see all of these issues coming together and cloud computing playing a key role in accelerating the outcomes sought by the Government in its Digital India vision. We therefore recommend TRAI to also provide leadership and restraint in helping to create a transparent and trusted regulatory environment for India's cloud products and services.

Key points in the response:

1. Cloud computing is a holistic term encompassing ICT infrastructure, processing, storage, networks, operating systems and applications that are available *on demand* in variable quantities. Cloud computing fundamentally transforms the economics of ICT usage by transferring the focus of ICT consumption away from capital expenditure to operational expenditure. A cloud-based business model enables stronger budget control and greater agility in financing requirements and therefore growing a business.
2. Cloud computing encourages customers to develop a *DevOps* culture – an organizational culture characterized by continual exploration and development of new services and operations that can automate, enhance or otherwise improve service delivery. With *elastic computing* provided by the cloud, system operators and engineers at any company at any time have access to the tools needed to explore new solutions on a continual basis without the need for purchasing and provisioning expensive, in-house servers and computers.
3. The agility enabled by the cloud computing model allows businesses to be able to profit from highly variable demand. It is this that is fundamental to the cloud business model and it is what is fuelling the rapid expansion of new services and enabling a new wave of innovation.
4. Customers will choose cloud service providers based on their ability to enable growth (the time it takes to scale up access to services or provide the necessary support), on service reliability (including risk management and technical assurance), and on cost control. None of these are areas that respond well to regulation or government mandate. Because customers will also often need agility in terms of support for different operating systems, programming languages, and so on, this is leading to different approaches by cloud service providers in developing the market, with the result being a rich and varied market environment.
5. When data and computer systems are moved to the cloud, responsibilities become shared between the customer and the CSP. The level of responsibility on both parties depends on the cloud deployment model type, and customers should be clear as to their responsibilities in each

model. Typically the CSP will be responsible for securing the underlying infrastructure that supports the cloud, and the customer will remain responsible for the data that is put into the cloud. This shared responsibility model reduces operational burdens in many ways, but it also means that, as the data owner, the customer retains control and ownership over their data.

6. Where government regulation has a role to play is in providing a clear regulatory environment for data privacy such as a data privacy act. With adequate personal data protection provided for in law, there should be no need for additional provisions mandating data control on the cloud. Cloud services should be considered a business without further need of licensing, as this may have the impact of slowing cloud development and adoption if overly-onerous requirements are introduced.

Detailed Responses on the Consultation Paper

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

a. Accelerating the design and roll out of services

Cloud computing is a holistic term that encompasses ICT infrastructure, processing, storage, networks, operating systems and applications that are available on demand in variable quantities. Cloud computing fundamentally transforms the economics of ICT usage by transferring the focus of ICT consumption – and therefore cost – from capital expenditure (CapEx) to operational expenditure (OpEx). Thus where capital intensive expenditures depreciate over time, a cloud-based OpEx budget allows for stronger budget control and greater agility in financing ICT requirements and therefore growing a business.

Customers only need to pay for the ICT resources that they use, as opposed to in-house ICT environments where resources must be purchased and installed in fixed quantities based on an estimate of future demand. On-demand computing resources allows the cloud user to adjust the amount of ICT available without the need to wait for budgeting, procurement, instalment, configuration and testing. This model of *elastic computing* allows the cloud user to scale up or scale down the service provisioning nearly instantly. New services can be tested and rolled out without delay, and the cloud customer only pays for the ICT resources that they utilize.

Cloud computing thus encourages customers to develop a *DevOps* culture – an organizational culture characterized by continual experimentation and development of new services and operations that can automate, enhance or otherwise improve the cloud customers' service delivery. With *elastic computing* provided by the cloud, systems operators and engineers have access to the tools needed to explore new solutions on a continual basis without the need for purchasing and provisioning expensive, in-house servers and computers.

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

E-commerce and social networking have been at the vanguard of digital economy developments in many countries across the globe, with e-commerce start-ups being able to have multinational and export businesses from the moment they launch because of increased reach and competitive costs. Participative governance and social inclusion have similarly formed the backbone of emerging digital programs enabling governments to reach citizens and offer services that were previously deemed uneconomic.[4]

The computing resources needed to support social networking and two-way communications for participative governance, as well as for e-commerce, can be highly unpredictable and subject to rapid increases in demand for very short amounts of time. To be successful and sustainable, networking platforms must be able to support rapid growth while maintaining a competitive infrastructure and manpower cost base – especially in start-up and early growth phases. This is exemplified by the platform Slack (a US-based messaging application for teams), which grew to 1.1 million daily users and more than 30 million messages per week within 18 months of their launch. Such growth was only possible with the support of a flexible and highly scalable infrastructure that kept costs down in the start but that could

[4] See GSMA (2016) "Advancing Digital Societies in Asia" https://www.gsmaintelligence.com/research/?file=9f48d32ff0671fb7dbbcb4efb84eabc0&download; and TRPC (2015) "Going Digital: The Status and Future Potential of Internet-Based Economies in Asia" http://trpc.biz/goingdigital-asia-workshops/

deploy new resources rapidly when and as the service gained popularity. With on premise ICT, Slack would have needed months to add the necessary capacity; by utilizing the cloud, they were able to deploy new servers as and when they were needed, typically within 30 seconds.[5]

When demand for a particular good or service on an e-commerce portal, or the desire to access or comment on a particular piece of information, *goes viral*, the demand for network capacity and computing resources to support the underlying applications grows rapidly. In-house ICT resources are unlikely to be able to support such sudden spikes in demand. To provision in-house resources that can support such demand will be costly, and will involve significant over-provisioning in times of low demand. Interflora (a flower delivery company) exemplifies this utility of the cloud; their cloud-based e-commerce platform allows them to handle seasonal spikes in flower orders, such as for Valentine's Day, allowing platform updates continuously.[6]

Cloud services enable users to meet unexpected spikes in demand – as well as rapid growth over time – for ICT resources. Credible CSPs can deploy additional resources within seconds to meet this demand.

Cloud computing enables participative governance. It enhances transparency – both in costs as the billing runs almost like metered utility with granular usage details; and in providing visibility into ICT resources that have been provisioned, their utilization and complete traceability of identity and access. All at the click of a button on a consistent basis.

c. Expansion of new services.

Cloud software and services enables access to enterprise-grade tools that would simply be too costly to procure using an in-house environment.

The agility of a CSP in being able to meet the highly variable demands of users is fundamental to the cloud business model and is what is fuelling the rapid expansion of new services. Customers will therefore often choose a CSP based on the time it takes to scale up access to services, such as the number of server instances. Customers often also need agility in terms of support, including for different operating systems or programming languages, for example. This is leading to different approaches by CSPs in developing the market. It is this market competition that ensures that CSPs continue to renew and innovate. Continued infrastructure upgrades by CSPs and releases of new features and services are a strong sign, and indicative the cloud environment is servicing a healthy and growing ecosystem.

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

Cloud services can enhance the efficiency of inter-agency collaboration. This is true for both government and enterprise. Agencies can share resources across departments, allowing for greater efficiency, entrepreneurship, and creativity in delivering public services. With centralized data storage, management, and backups, data retrieval and business recovery during times of crisis (e.g. natural disasters or other disruptive events) also become faster, easier and more cost effective.

Reducing the amount of ICT infrastructure required to be built, owned and maintained by agencies reduces overall deployment times, and shifts the focus from management of infrastructure to delivery of

[5] AWS, n.d., Slack Case Study https://aws.amazon.com/solutions/case-studies/slack/?pg=main-customer-success-page
[6] AWS, n.d., Interflora Case Study https://aws.amazon.com/solutions/case-studies/interflora/

services. Public ICT facilities and services can be tested and deployed quicker, and maintained more cost effectively, than if the agencies own and run unique computing facilities themselves.

The elastic computing model of cloud computing turns ICT resources into a utility, where the customer pays for what they use. This allows governments to purchase as much or as little resource as they need, when they need it. The utility-based pricing structure is also more transparent than bulky, irregular procurement contracts, which facilitates implementation of spending caps and greater budget control. Elastic computing is also beneficial for industries that need a tremendous amount of resources with a specific project, but not all the time. This includes, for example, clinical research applications, which involve large-scale data analysis and modelling. Pharmaceutical company Pfizer was able to realize vast cost savings by shifting their high performance computing services for research and development to the cloud. This enabled Pfizer to draw on cloud computing resources during peak computing loads without needing to invest in more hardware and software.[7]

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

Utilizing the cloud allows the customer to acquire infrastructure on-demand, which means the organization only pays for what they use. This contrasts to the traditional set-up of procuring ICT resources in-house, where resources must be purchased and installed in fixed quantities based on an estimate of future demand (see the figure in Question 1, above).

Reputable CSPs provision ICT on an enormous scale, and they realize savings from the resulting economies of scale. The marginal costs of installing and maintaining servers and other ICT resources for a CSP is negative – each additional server or application costs less to maintain than the previous one.

To take one example, and depending on location, a cloud customer could rent a server instance from AWS for less than USD0.70 per hour – about USD52 per month.[8] A customer needing 100 servers would therefore be paying USD5, 200 per month (given constant demand). In this example, procuring 100 servers in-house, *and including only the hardware costs,* would have cost the business an estimated 21% more over three years.[9] And this is without even beginning to consider labour costs. Nokia runs their mobile internet services platform on 2,200 servers through AWS, collecting in excess of 800 GB of data daily. At this scale Nokia struggled to manage their reporting in-house. Moving their data warehouse to AWS enabled Nokia to save around 50% on business analytics costs while data queries ran twice as fast.[10]

Economies of scale (and scope) are also generated through the facilitation of collaborative work processes. This can be cross-department, cross-silo, or cross-community. By enabling information and workload sharing where previously there was none, economies of scale become possible *at no extra capital cost*.

[7] AWS, n.d., Pfizer Case Study https://aws.amazon.com/solutions/case-studies/pfizer/?pg=main-customer-success-pagel
[8] AWS, 2016, How AWS Pricing Works https://d0.awsstatic.com/whitepapers/aws_pricing_overview.pdf
[9] Based on AWS' total cost of ownership calculator: https://awstcocalculator.com/. Configuration based on 100 servers, each with 4 processing cores, 32GB of memory and 1,000GB storage.
[10] Nokia Case study. Available at: https://aws.amazon.com/solutions/case-studies/nokia/?pg=main-customer-success-page

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?**

A lot of companies, including Indian companies and especially SMEs, have begun the move to IT and digitization. Cloud computing can make this move easier, cheaper and faster because there is no need to procure ICT management skills in-house.

Procurement of cloud services will depend on a range of considerations, including:

- the hosting and computing requirements of the business and/or service offering
- the total cost of ownership of the services
- pricing approach, philosophy and history
- the experience and footprint of the CSP
- agility of the services
- pace of upgrades and innovation
- the technical refresh budget
- the service breadth, depth and software ecosystem
- security, privacy, and audit
- vendor lock-in

Broadly speaking, these issues can be grouped into three buckets:

1. **Helping businesses scale rapidly**

Cloud computing enables agility and nimbleness by outsourcing the capex requirements of the business's ICT setup. A core focus for businesses looking at deployment models is thus how to use the tools available to increase responsiveness. Different cloud customers will require different support in terms of, for example, programming languages, operating systems, database handling and applications. Some customers may need Linux-based virtual machines to install and manage their own applications; other customers may need broad support for programming in different languages; some customers need support for a specific type of data storage, while other customers need effective integration of in-house ICT systems with the cloud infrastructure.

2. **Lowering cost, increasing effectiveness**

Some customers will prioritize cloud solutions that offer variable pricing based on usage. For price-sensitive customers, the pricing history of the CSP may therefore be an important factor. Pricing transparency in this case will be paramount. While most cloud customers will typically prefer utility-based pricing models (shifting ICT expenditure from CapEx to OpEx), very large customers in some cases may prefer fixed pricing models. Regardless of pricing preference, cloud customers will look to use cloud services to reduce their total ICT-related costs and increase their business effectiveness.

3. **Providing assurance**

A third set of considerations revolve around the security approach of the CSP, data privacy considerations, auditing and so on. Cloud customers may have specific requirements in terms of data security. In all cases the customer should look to industry certifications and accreditations using international standards for assurance that the CSP's security frameworks, privacy policies and other risk-related concerns meet the customers' needs.

Between enterprises and SMEs the emphasis on these 'buckets' will often differ with larger enterprises focusing initially on cost control measures for mass usage and assurance, while SMEs will tend to emphasize the ability to rapidly grow their business reach and operations. Such decisions are not either/or, but will often be a combination of factors depending on the scale, maturity and operations of the business. Larger enterprises may prefer to procure cloud services from CSPs that offer specific types of ICT services, such as compute-optimized, memory optimized, or storage-optimized services. SMEs are more likely to procure service that are primarily cost-effective.

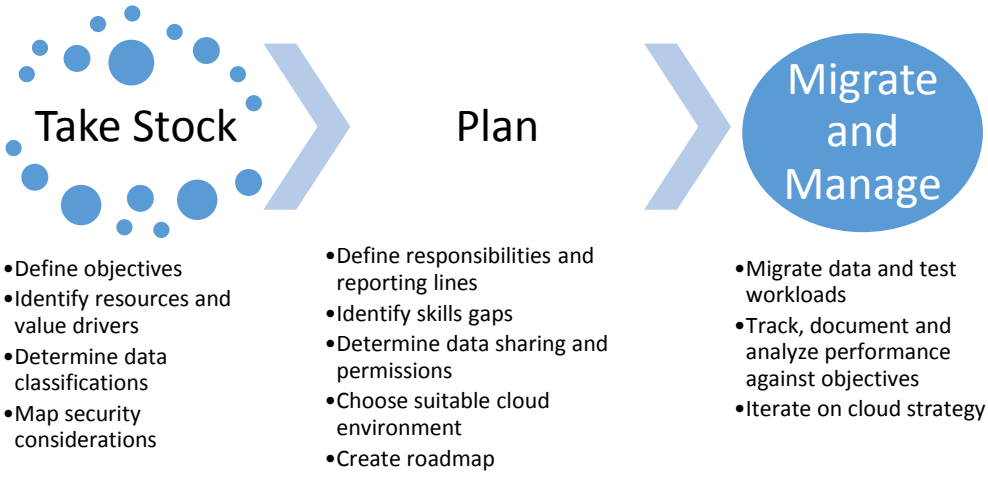
A key transformation that has been enabled by the advent of cloud computing is the affordable access to enterprise-grade tools for SMEs, tools that that would simply be too costly to procure using an in-house environment and were therefore previously out of reach until a business reached a certain size and scale.

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?

Migrating data into or between cloud environments should always remain within the control and the responsibility of the data owner.

Cloud services can be expected to be able to integrate with existing services and be interoperable with locally provisioned ICT. Contracted cloud services should also preclude vendor lock-in and enable the customer – the data owner – to transfer data and applications from one cloud environment to another. This remains the responsibility of the data owner.

Customers migrating data and workloads to the cloud, or between different CSPs should always follow a three-step process to ensure secure migration: (1) Take stock (2) Plan (3) Migrate and manage.



1) Take stock
Take stock of data to be migrated, including as required the relevant data classifications and corresponding security considerations. Non-sensitive workloads and those that pose low security concerns can be migrated using common transfer protocols and services, while sensitive data may require a bespoke approach to migration.

The value of moving workloads to the cloud is determined by the technology lifecycle and the increased functionality that cloud can bring. Moving workloads from IT resources that are near the end of their current technology lifecycle can avoid costly investments in new IT resources.

2) Plan
A roadmap for migrating data and workloads should be developed, including defining responsibilities and reporting lines. Migrating workloads to the cloud can change the skills needed within an organization, for example by requiring fewer people concerned with managing IT infrastructure. The cloud customer should work with their CSP to understand staff skills, training and education needed and to manage workloads post-migration.

- Identify data that can be shared, and would benefit from being shared, and requirements on security and access permissions for such data.
- Identify the suitable cloud environment, such as virtualization of legacy IT, performance and functionality requirements, costs, and compatibility with legacy IT.
- Determine whether replacing existing applications with new ones or redesigning service delivery architecture from the bottom-up is preferred.

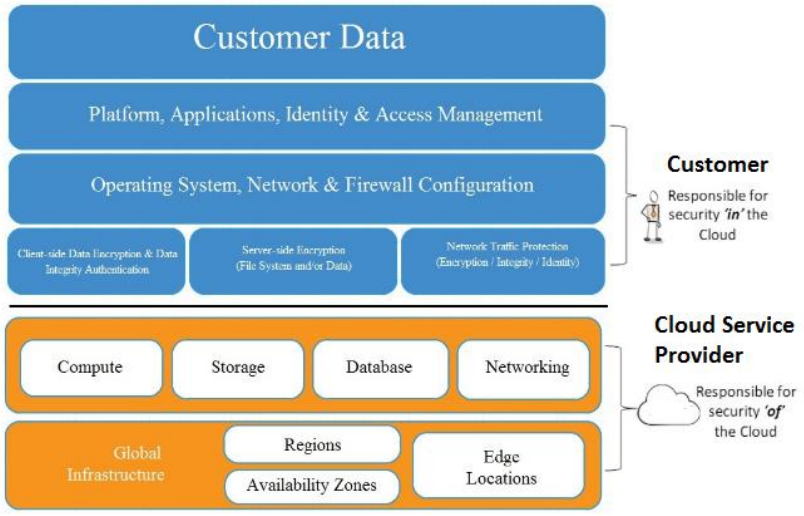
3) Migrate and Manage
The cloud customer should track, document and analyse progress of their migration plan in an iterative manner, monitor performance and service delivery against their objectives, and compare costs against their migration plan. Post-migration, testing of the new, cloud-based environment should always be performed before decommissioning existing ICT solutions. This is important in avoiding glitches post-migration. Testing should be performed on the basis of both typical/normal usage scenarios and extraordinary utilization/demand scenarios.

All of these steps will be handled by, and under the control of, the customer when using a self-service cloud platform.

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?

When data and computer systems are moved to the cloud, responsibilities become shared between the customer and the CSP. The level of responsibility on both parties depends on the cloud deployment model chosen, and customers should be clear as to their responsibilities in each model. AWS uses a Shared Responsibility Model in which AWS is responsible for securing the underlying infrastructure that supports the cloud, and the customer remains responsible for the data that is put into the cloud. This shared responsibility model means that, as the data owner, the customer retains control and ownership over their data at all times.

A sample Shared Responsibility Model is depicted below:



Three key points are paramount:

1. The customer should retain ownership of its content.

2. Any regulatory provisions should take account of the cloud service delivery models wherein the customer retains control of its content, including during movements in and out of the cloud. Trying to define an allocation of control and responsibility with a with a 'one size fits all' approach will be counterproductive as there are multiple service delivery models in the industry, each defined by different allocations of control/responsibility between the customer and CSP based on the actual service in question.

3. CSPs should not access or use customer content except to provide and maintain the cloud services or as legally required.

Where government regulation has a role to play is in providing a clear regulatory environment for data privacy such as a data privacy act. With adequate personal data protection provided for in law, there should be limited need for additional provisions mandating data control specifically for the cloud.

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?

A major benefit of cloud computing as compared to traditional IT infrastructure is that customers have the flexibility to avoid traditional vendor lock-in, and CSPs should allow customers to move data on and off their cloud platforms as needed. However, regulating for such an outcome, particularly at such an early stage of industry development, is likely to inhibit innovation and slow local industry growth. Regulating for cloud computing interoperability is not something that has been undertaken elsewhere.

Internationally, much work has been done in various industry bodies to set standards or processes for promoting interoperability and the best way to ensure interoperability is therefore to adhere to the work already done by following industry best practices and, where they have been widely adopted, international standards. These include international standards such as the ISO/IEC 17203:2011 Open Virtualization Format (OVF) specification, for example.

To relieve the cloud customers of vendor lock-in, and associated risks such as higher procurement costs, the CSP should ensure that their services are reversible and that the customer controls migration both to and from the CSP's cloud platforms. Reversibility allows the customer to leave one CSP and move to another. The same processes that enable reversibility also enable convenient and secure migration to the cloud in the first place.

Data storage interoperability
The customer should be able to extract some or all of their data from the CSP. For multi-TB instances, the CSP can enable physical devices to be shipped to the CSP, upon which the CSP can export the data from cloud storage. The customer should also retain the ability to destroy their data on the cloud, for example by destroying the encryption master key.

Computing interoperability
Virtual machines on one cloud can be replaced by VMs on another cloud provided the language protocols and platforms are interoperable. The cloud customer decides which protocols and platforms they deploy onto the cloud infrastructure, or which cloud platforms they contract as a service. This allows the customer to ensure their platforms and associated APIs achieve their needs, and also allows the customer to choose services that are interoperable. Contractual arrangements that follow industry standards and best international practice increases the compatibility and interoperability of one cloud service with other cloud services.

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.

The cloud customer will decide on the deployment model they need in order to meet their needs and achieve their objectives. Successful cloud procurement strategies focus on application-level, performance-based requirements, rather than dictating the specific methods, infrastructure or hardware used to achieve performance requirements. Again, given the different cloud service models available and emerging, *mandating* QoS parameters can be counterproductive. Key QoS parameters focused on by customers to achieve their objectives are uptime and security and can include various other quality of service aspects which may then be stipulated in a procurement contract if so warranted.

Key Considerations for QoS
In addition to requirements in terms of uptime and security, the cloud customer may refer to a range of quality aspects when procuring cloud services. These aspects may include:

1) Experience

- How long has the vendor been providing cloud-related services?

- Can the vendor provide case studies that reflect their experience as a commercial cloud service provider?

2) Scalability and Global Footprint
   - How large is the vendor's global footprint?
   - Are you able to select where the workload/data is stored?
   - Do you have the ability to access hundreds of thousands of cores if needed?
3) Service Breadth and Depth
   - Provide details on flexibility, depth, and breadth of the services.
   - Can the vendor provide multiple types of compute instances (e.g., all-purpose, compute-optimized, memory optimized, storage-optimized, etc.)?
   - Are multiple programming languages (Java, PHP, Python, Ruby), operating systems (e.g., Windows, Linux), databases (e.g., SQL, Oracle) and widely used applications (e.g., SAP) readily available?
   - Is there highly durable storage for all types of data?
   - Are there options for integrating existing on-premises infrastructure with the cloud provider?
4) Partner and Software Ecosystem
   - How extensive is the ecosystem of partners that have expertise and experience architecting, providing, and building solutions using the vendor?
   - Is there a marketplace of ready-to-go third-party application solutions?
5) Security, Privacy and Audit
   - Does the Cloud Service Provider (CSP) leverage industry-acknowledged best practices, certifications, and accreditations that demonstrate security, privacy, and other capabilities?
   - What is the extent of those certifications and accreditations?
   - Does the CSP have Federal Risk and Authorization Management Program (FedRAMP) certification from the US government?
   - Does it have the resources to be a leader in the marketplace to continue to maintain, enhance, and grow these capabilities?
   - Ability and costs of vendor to implement prescribed certifications.
6) Industry Analysis
   - How is the provider assessed/positioned by independent analysts?
7) Government
   - Definitions of Cloud
   - How does the CSP meet internationally accepted standards on various deployment and utilization models for IaaS, Platform as a Service (PaaS), and Software as a Service (SaaS) offerings?

8) Vendor Lock-In

- What is the extent of lock-in with the cloud provider?
- Can you remove your data/applications at any time?
- Are there minimum commitments required to use the infrastructure (e.g., one year of guaranteed usage)?

9) Pace of Innovation

- How does the vendor continue to innovate its offerings to keep pace with the rapidly changing world of information technology?
- What is the vendor's published history of providing innovative new services and feature upgrades to existing services?
- How rapidly can the infrastructure provider implement innovative and updated features, upgrades, and services?
- How are these innovations translated into usable features in the cloud?

10) Technology Improvement and Refresh Methodology

- Is there methodology for the cloud service to refresh and upgrade offerings?

11) Agility

- How agile is the access to the CSP's offerings?
- How flexible are the CSP's service offerings? What options are there for different operating systems and programming languages?
- Is the infrastructure design locked-in?
- How long does it take to get access to a specific service (e.g., how quickly can a server instance be spun up)?

12) Pricing Approach, Philosophy and History

- Does the vendor provide variable, utility-based pricing?
- What is the history of price reductions?
- Is there any variability to the pricing?
- Is the pricing fully and publicly transparent?
- How granular and flexible is the available pricing?
- Can the service be used in an Operational Expenditure (OpEx) budgeting type model (as opposed to Capital Expenditure [CapEx])?
- Are prices for services locked and/or required for an extended period of time (e.g., a flat monthly price for the length of the agreement)?

13) Technical Refresh Budget

- Does the pricing for using the cloud provider include continual technical refresh of offerings?
- What is the history of providing new and updated services and capabilities?

14) Total Cost of Ownership (TCO)

- Can the CSP provide a Total Cost of Ownership (TCO) estimate of your offering vs. a traditional offering?

Customers should rely on best practices and third-party accreditations for assurance that the CSP can deliver the desired quality of service, as opposed to dictating the use of specific equipment or procedures (e.g. racks, server types, etc.). By leveraging commercial cloud industry-standards, customers avoid placing unnecessary restrictions on the services they can utilize, and avail access to the most innovative and cost effective cloud infrastructure solutions.

Contract Vehicles for Different Service Models
Different cloud services providers can be measured differently, according to the contract vehicles through which they have been engaged. There are effectively two types of contract vehicles: direct or indirect:

- **Direct Purchase from CSP** – Use terms designed for a commercially available service. Purchased as a commercial item service that is offered without labour hours.
- **Indirect Purchase from a CSP Partner** – Purchased from a CSP partner/reseller, negotiating an agreement with that organization.

Service Models: Managed vs Unmanaged Services
It is also important to recognize the difference between purchasing cloud infrastructure and managed services.

- "Unmanaged" Cloud Services – Cloud infrastructure and platform services, purchased as a commercial item service from a CSP.
- "Managed" Services – Firms that help customers design, architect, build, migrate, and manage their workloads and applications on the cloud.

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?

Cloud services should be billed using a utility model for ICT resources, whereby customer usage is metered on the basis of their usage of computing power, storage, other related services, and data transfer over the network. The customer should be billed on the basis of agreed pricing models for the usage of these ICT resources.

The CSP will usually provide usage metering and usage reports for each type of cloud service provided to the customer. The customer will therefore be able to assess usage by type and over different timeframes in real time, including real time usage and customized reports generated on demand. This will allow the customer to monitor their usage, which of their applications or purposes are generating what volume of usage, as well as usage over different time periods in order to assess demand baseline and usage spikes. In the event of dispute, the customer should therefore be able to monitor and check their consumption.

To avoid unexpected charges the customer can monitor usage charges using alerts and notifications. Billing alerts can notify the customer when their usage reaches or exceeds the thresholds that have been

defined by the user. Such alerts can be sent to the customer via appropriate notification channels. Customers can also be enabled to sign up for alerts when there are changes to the pricing of services that the customer has contracted and/or when new services are launching.

One of the distinctive advantages of cloud computing is real time usage monitoring and greater control therefore over forecasts for current and future billing cycles based on past costs. Usage metering can for example graph spending on the cloud services that the customer uses the most, including their proportion of total costs. Often a CSP will provide a knowledge depository or "knowledge center" that covers a comprehensive set of questions and answers about metering and billing. In the event then that the customer does not understand their metering, usage report or billing, this provides a convenient first stop for the cloud customer, and can serve as a good awareness and assurance tool as customers transfer to the cloud and in building greater comfort and familiarity with this strength of the cloud computing model. A customer support center can also be a boon in assisting customers with billing inquiries. (See also Question 9, below.)

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

In the first instance, customer complaints and grievances will best be handled by CSP helpdesks or account managers, as this remains a service issue. Disputes that cannot be resolved through this process should be resolved through traditional escalation processes.

Various methods of external communication will typically be implemented to support customers' complaints, including information posting on the CSP's website, through customer support phone lines or other electronic means email, messaging and video conferencing.

Mechanisms will likely also be in place to allow the customer support team to be notified of operational issues that impact customer experience. One example is the use of a "service health dashboard" through which the CSP's customer support team is able to alert customers to issues that may be of broad impact or interest. Within this context a "security center" would be able to make available security and compliance details about the CSP. Similarly, CSPs will often provide simple, real-time access to usage statistics giving a further ability to define notifications based on particular triggers.

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.

The security of any ICT environment depends on the appropriate application of physical and logical security controls. In a cloud-based ICT environment, the overall security can be enhanced by outsourcing the physical security controls to the CSP while retaining control over logical security controls.

Physical security controls comprise three aspects:

- Restrict physical access to the ICT infrastructure to those persons that have appropriate permissions;

- Ensure that the ICT infrastructure is safe from physical and environmental risks, such as flooding and will remain operational, or resume operation within an accepted delay, in case of e.g. loss of electricity;
- Monitor physical and environmental controls and notify when related events occur.

Logical security controls comprise protocols and tools to prevent modification, disclosure, loss, or misuse of data by a malicious actor, such as but not limited to:

- Defining security clearances for different data classifications;
- Defining security standards and users' authorization levels;
- Managing data according to the data classification;
- Implementing and operating software-defined identification and authentication of individuals accessing data.

In a cloud-based ICT environment, the customer retains a commensurate if not greater level of control and ownership over their information as an on-premise environment, but responsibility for the control framework changes. The cloud customer configures security features based on a risk assessment and decides which security controls are appropriate for the different data they migrate to the cloud.

For a cloud-based ICT environment, physical security controls are managed by the CSP. CSPs typically have stricter physical access controls than what can be feasibly implemented for in-house ICT. A CSP's data centers will also typically have far more robust protections against environmental threats and human error. CSPs can also provision rapid or on-demand scaling of the ICT resources that are available – where it would typically take days, weeks or months to scale up an in-house ICT system. As a result, the physical security controls in a cloud-based system are more robust than on premise ICT environments.

The cloud customer should refer to international standards to validate procedures for the physical security of their data. Ensuring that the CSP complies with international cloud and information security standards, such as e.g. the Service Organisation Controls (SOC) 1, 2, and 3 reports or the International Organization for Standardization's ISO/IEC 27001[11] for information security management systems, gives the cloud customer assurance that the cloud infrastructure they are using is secure. CSP compliance with international standards should be audited by an independent third party.

By referring to international standards and third-party compliance audits, the cloud customers can be confident that their contracted cloud services meet their requirements for security and reliability.[12]

The control framework of a cloud customer should focus on logical controls:

- Data classification and data handling standards, with minimum security requirements for each classification (e.g. *public, confidential*, and *secret*);
- Defining and monitoring data access controls for the cloud platforms and applications;
- Implementing and operating appropriate data management and encryption;

[11] http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
[12] UK Cloud Service Security Principles (Beta), see: https://www.gov.uk/government/publications/cloud-service-security-principles/cloud-service-security-principles

- Preventing risks associated with software security, including procedures to ensure operating systems and software are up-to-date;
- Managing personnel security, including staff training and procedures for reporting misconduct and revoking data access;
- Monitoring cloud performance; and
- Continuity planning, incident handling and event logging.

Data classification

The control framework depends on effective classification of new data. The person or team responsible for classifying new data should perform a risk assessment for data that is being generated by the organization. Depending on the institutional or business risk that is associated with the data, and the value, sensitivity and criticality of the data, the data is classified into the appropriate category.

The minimum required security depends on the data classification and risk assessment. The cloud customer should define access controls and minimum security requirements for the handling and management of data within each data classification.

Restricted, confidential or secret data will require more rigorous security controls, while non-restricted and non-sensitive data will require basic security controls. In defining the required security standards, the cloud customer should, as far as possible, make references to international standards such as ISO 27001 for information security management systems, [13] ISO 27017 on cloud-specific information security controls,[14] and ISO 27018 on protection of personally identifiable information on public clouds.

CSPs implement security standards with reference to international standards. By referring to international standards in the definition of minimum security standards for each data classification, the cloud customer can more readily assess which cloud services provide assurance to the level of information security and control that they require.

Assigning security requirements based on data classifications can reduce the cost of data management for the organization, facilitate more efficient usage and sharing of information within the organization and between different organizations, and will help ensure that data is appropriately secure.

Defining and monitoring access controls for the cloud platforms and applications

While physical security controls are managed by the CSP, the cloud customer retains control of the definition and management of access controls. The cloud customer grants, manages and revokes data access permissions as necessary, and is responsible for ensuring permissions are kept up-to-date.

The person or team responsible for access permissions must actively manage data access lists such that data resources are available to those that need the data – e.g. to perform their work duties or as a matter of right-to-access public information. They must also manage lists such that people that are not supposed to access certain data are not able to access the restricted data.

[13] International Standards Organisation, n.d. ISO/IEC 27001 - Information security management http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

[14] ISO27001Security, n.d., ISO/IEC 27017:2015 / ITU-T X.1631 — Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services http://www.iso27001security.com/html/27017.html

The cloud customer also controls how data is being used. This includes deciding what operating systems and software are used to manage the data on the cloud (see below).

Implementing and operating appropriate data management such as encryption
Data should be transferred, stored and processed according to the security requirements of its classification. Depending on classification, this typically includes ensuring the confidentiality of data by encrypting data "at rest" and by encrypting individual files or the entire drive where the files are stored.

The cloud customer can control where the data is being stored, including choosing the jurisdiction where the data is located. Cloud customers that transfer personal information or other data that is subject to restrictions on cross border data transfers must ensure their data is stored and processed by a CSP that offers the necessary certifications and requirements. For example, a cloud customer transferring data from the EU to India will benefit from using a CSP that offers a Data Processing Agreement incorporating the Model Clauses which has been approved by the European Article 29 Working Party.

The cloud customer also controls *how* data is being transferred and stored. This includes deciding whether data needs to be encrypted from end-to-end or only encrypted while it is stored[15], whether data masking is necessary, which creates similar but inauthentic versions of the original data before it is transferred and processed, and whether data needs to be anonymized by stripping all personal identifiers from the data before being transferred or processed.

Preventing risks associated with software security
The cloud customer retains control and responsibility for operating systems and software that they install on the cloud. The cloud customer must therefore continue to implement procedures for regular installation of updates and security patches for operating systems and software applications running on the cloud.

Operating systems and software on the cloud that are not up to date are vulnerable to data breaches by unauthorized third parties in the same way that operating systems and software on in-house ICT systems are. The cloud customer should manage all applications and tolls that they install on the cloud according to the same security procedures that they use for local servers and workstations.

Customers that build applications in the cloud should take the opportunity to incorporate secure software development practices to ensure the applications that they build are robust and that their attack surfaces are minimised, thus reducing the risk of compromise by malicious actors.

Managing personnel security
The cloud customer should screen and monitor employees and personnel that have authorized access to their cloud services the same way they monitor employees with privileged access to in-house resources. Cloud customers should therefore consider personnel security a key component of their overall security control framework.

[15] Data will typically be encrypted "in motion" by using encrypted channels for transferring data. For web-based transfers, this implies implementing encryption using a third-party certificate from a trusted vendor – which results in the "s" in "https" that you see on web-addresses such as https://www.domain-name.com. Increasingly, there is no reason not to a secure, encrypted channel for transferring data – the impact on performance is negligible and your data is more secure.

To manage personnel security risks, the cloud customer should focus on robust screening of new employees, implement employee reviews to continually assess employees' continued employment, and conduct security and incident reporting training where appropriate. Personnel security management helps protect the people, information and assets of the organization.

Monitoring cloud performance

Once security controls have been defined and implemented, the cloud customer should monitor cloud performance to ensure the continued effectiveness of the implementation of the security controls.

The cloud customer can monitor and log connections and data access. The UK Government's Cloud Service Security Principles illustrates how an organization with a cloud policy can manage and monitor the effectiveness of the security controls, and the requirements upon CSPs to provide cloud customers with the tools to do so in an effective manner:

- Customers should be provided with the tools required to help them securely manage their service.
- All external or less trusted interfaces of the service should be identified and have appropriate protections to defend against attacks through them.
- Customers should be provided with the audit records they need to monitor access to their service and the data held within it.[16]

To implement an effective monitoring framework, the cloud customer needs to define roles within the organization. Each aspect of defining, implementing and monitoring the components of a control framework need to be delegated to specific individuals or teams.

- Who is responsible for classifying new data?
- Who is responsible for managing the data?
- Who is responsible for managing access permission?
- Who is responsible for monitoring and reporting on cloud service performance?

The respective individuals and teams should report to and coordinate their overall approach under one clearly defined representative in senior management.

The person or team that is responsible for monitoring cloud performance should ensure they have access to the necessary tools and logs to monitor aspects of cloud performance such as service availability, network performance, data access and data breaches. The cloud customer should compare performance against their demands and report regularly to budgeting and management committees. In this way, cloud ICT resources can be managed and evaluated the same way other utilities and outsourced services are, and the ICT strategy can be improved over time to match the organization's need. This can also help the organization continue to explore new uses of ICT to develop new or better services.

In parallel to cloud performance management, the cloud customer should take note of cloud asset usage and actively manage its cloud assets. The increased agility and rapid deployment of cloud services as compared to in-house ICT means that the cloud customers' ICT policy should be informed by active

[16] UK Cloud Service Security Principles (Beta) https://www.gov.uk/government/publications/cloud-service-security-principles/cloud-service-security-principles

management of cloud assets. Well-informed decisions about cloud procurement will help align cloud resources with the needs and goals of the organization.

Continuity planning, incident handling and event logging

Cloud customers perform business continuity planning to ensure that information and data are available to the user, whereby the need for constant ICT services availability is balanced against the cost of provisioning automatic fail-overs and redundant systems. For non-critical services, the short-term absence of which is unlikely to lead to critical loss, the cloud customer may be willing to not provision redundant ICT systems in case of a loss of access. For critical services, the organization may choose to procure cloud services with redundancy built in, or deploy a hybrid ICT system where some services are provided for in-house.

Regardless of the system design, incident handing and event logging is a critical component to minimize the risk of loss related to service outages and other security related events. The cloud customer should define clear roles and responsibilities in the event of loss of data, service outages and security breaches, and all authorized personnel employees know the key reporting contacts within the organization.

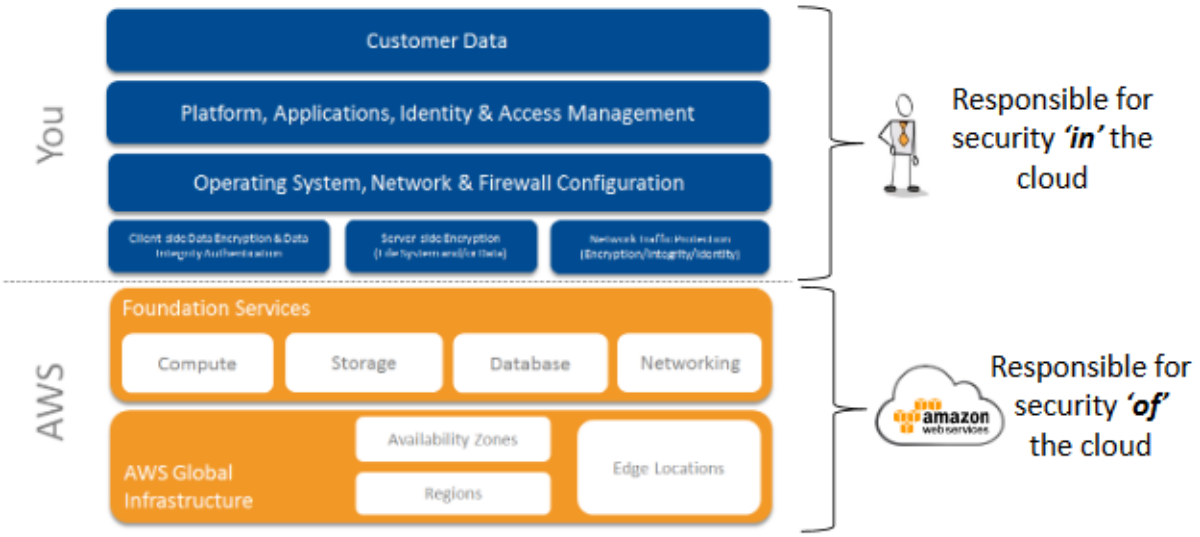
11. What are the termination or exit provisions that need to be defined for ensuring security of data or information over cloud?

Termination provisions are not a feature to be defined externally to the CSP-customer relationship as they will be defined by the contracted relationship between the CSP and the customer. Security commitments should last for as long as the relationship lasts. Any regulatory provisions would therefore need to take account of service delivery models wherein the customer retains control of their content and makes their own choices about migration to and from the cloud platform.

The responsibility for ensuring security of data and information over the cloud is a shared responsibility between the CSP and the customer. Both have a responsibility to ensure that there are adequate measures put in place to ensure infrastructure security (CSP responsibility), and safety with regard to management of accessing and moving data (customer responsibility.)

This shared responsibility becomes particularly important during termination and/or exiting a cloud vendor relationship, as termination or exit can be handled autonomously by the customer.

AWS Shared Responsibility Model



Customer Responsibilities

In this model the customer should understand their roles and responsibilities regarding secure data erasure, which are part of the controls "in" the cloud (as seen in the diagram above). Clients retain control and ownership of their data, and it therefore remains the customer's responsibility to manage the security of data in the process of termination and exiting a cloud contract. AWS in this instance would operate, manage and control the components from the virtualisation layer and underlying host operating system down to the physical security of the facilities in which the AWS services operate.

The customer is responsible for management of the guest operating system (including updates and security patches to the guest operating system) and associated application software, as well as the configuration of the AWS provided security group firewall and other security related features. The customer will generally connect to the AWS environment through services the customer acquires from third parties (for example, internet service providers). AWS does not provide these connections, and they are therefore part of the customer's area of responsibility. When exiting any cloud arrangement, customers should consider the security of these connections and the security responsibilities of such third parties in relation to their systems.

CSP Responsibilities

The CSP will provide the customer with the ability to delete data, along with information on the CSP's storage decommissioning process. As part of AWS's storage decommissioning process, for example, when a storage device has reached the end of its useful life, AWS procedures include a decommissioning process that is designed to prevent customer data from being exposed to unauthorized individuals. AWS uses the techniques detailed in the DoD 5220.22-M ("National Industrial Security Program Operating Manual") or NIST 800-88 ("Guidelines for Media Sanitization") to destroy data as part of the decommissioning process. All decommissioned magnetic storage devices are degaussed and physically destroyed in accordance with industry standard practices.

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

The overall process for data migration should follow the process outlined in Question 4, above.

The cloud customer should look to procure services from CSPs that can demonstrate that they meet the customer's security requirements. This is most effectively done by relying on third-party certifications and standardized tools and procedures for auditing certifications. For government agencies, this includes the CSP meeting the security requirements for government cloud accreditation; for commercial customers, verified against international cloud security standards is preferable. De facto international security standards include ISO 27001, Service Organization Controls Report (SOC) 1 and 2, Payment Card Industry Data Security Standard (PCI DSS), and Cloud Security Alliance (CSA) certification and audit. Data will be encrypted using industry-tested and accepted standards and algorithms, such as AES (128 bits and higher), 3DES (minimum double-length keys), RSA (1024 bits or higher), ECC (160 bits or higher), and ElGamal (1024 bits or higher).

The customer retains control over their data and should plan their migration around their data protection requirements, including restrictions on cross-border data transfers. Customers should migrate their data only when the CSP can provide assurance that they meet the customers' security and regulatory compliance requirements. If certain data classified as restricted require isolated storage, the cloud customer should not migrate this data to a shared host. Likewise, the cloud customer should ensure that live migration of their workloads does not move their data to an unknown location.

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

Cloud security is always a shared responsibility between the CSP and the end user. The level of responsibility on both parties depends on the cloud deployment model type, and agencies should be clear as to their responsibilities in each model. One recommended way to look at this shared security model is as below, where the end user takes care of the security controls "in" the cloud, and the CSP takes care of the security "of" the cloud (see diagram in Question 11, above).

CSP Responsibility: In a cloud-based ICT environment the CSP manages the physical security controls and all components up to the host operating system and virtualisation layer. CSPs typically have stricter physical access controls than what can be feasibly implemented for in-house ICT. A CSP's data centers will also typically have far more robust protections against environmental threats and human error, as well as failover switches that automatically provision redundant resources if a network resource fails. CSPs can also provision rapid or on-demand scaling of the ICT resources that are available – where it would typically take days, weeks or months to scale up an in-house ICT system. As a result, the physical security controls in a cloud-based system are more robust than on-premise ICT environments.

End User Responsibility: In a cloud-based ICT environment, the customer retains a commensurate if not greater level of control and ownership over their information as in a traditional, in-house ICT environment, but the responsibility for the control framework changes. The cloud customer configures security features based on a risk assessment and decides which security controls are appropriate for the different data they migrate to the cloud.

Thus, while physical security controls are solely managed by the CSP, the cloud customer retains control of the definition and management of access controls. The cloud customer grants, manages and revokes data access permissions as necessary, and is responsible for ensuring permissions are kept up-to-date.

In an AWS environment the customer is also responsible for management of the guest operating system (including updates and security patches to the guest operating system) and associated application software, as well as the configuration of the AWS provided security group firewall and other security related features. Operating systems and software on the cloud that are not up to date are vulnerable to data breaches by unauthorized third parties in the same way that operating systems and software on in-house ICT systems are. The cloud customer should manage all applications that they install on the cloud according to the same security procedures that they use for local servers and workstations.

The cloud customer also controls *how* data is being transferred to the cloud and stored. This includes deciding whether data needs to be encrypted from end-to-end or only encrypted while it is stored[17], whether data masking is necessary, which creates similar but inauthentic versions of the original data before it is transferred and processed, and whether data needs to be anonymized by stripping all personal identifiers from the data before being transferred or processed.

The customer will generally connect to the AWS environment through services the customer acquires from third parties (for example, internet service providers). AWS does not provide these connections, and they are therefore part of the customer's area of responsibility. When exiting any cloud arrangement, customers should consider the security of these connections and the security responsibilities of such third parties in relation to their systems.

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?

Cloud customers retain control and ownership over their data and have the ability to choose the geographic location(s) in which to store their data, with CSP identity and access controls available to restrict access to customer infrastructure and data.

Data Location

CSPs should provide customers with a choice as to how they store, manage, and protect their data, and not require a long-term contract or exclusivity. The cloud customer should procure cloud services where the customer retains control over where the data is being stored so that the cloud customer understands which jurisdiction their data is subject to and the rules by which their data can be accessed – e.g. by government authorities.

[17] Data will typically be encrypted "in motion" by using encrypted channels for transferring data. For web-based transfers, this implies implementing encryption using a third-party certificate from a trusted vendor – which results in the "s" in "https" that you see on web-addresses such as https://www.domain-name.com. Increasingly, there is no reason not to a secure, encrypted channel for transferring data – the impact on performance is negligible and your data is more secure.

AWS data centers are built in clusters in various global regions. We refer to each of our data center clusters in a given country as a "Region." Customers have access to thirteen AWS Regions around the globe. Customers can choose to use one Region, all Regions or any combination of Regions. The figure below shows AWS Region locations:

AWS customers choose the AWS Region or Regions in which their content and servers will be located. This allows customers with geographic specific requirements to establish environments in a location or locations of their choice. For example, AWS customers in India can choose to deploy their AWS services exclusively in the India Region, if this is their preferred location. If the customer makes this choice, their content will be located in India unless the customer chooses to move that content. AWS only stores and processes each customers' content in the Region(s), and using the services, chosen by the customer, and otherwise will not move customer content except as legally required.

Transfer of personal data cross border

When using AWS services, customers may choose to transfer content containing personal data cross border, and they will need to consider the legal requirements that apply to such transfers.

Examples of data lifecycle stages, disclosure examples, and considerations

Data Scenario	Summary	Considerations
Collecting personal data	It may be appropriate or necessary to inform individuals (data subjects) or seek their consent before collecting their personal data. This may include notification about the purpose for which their	Customer: The customer determines and controls when, how and why it collects personal data from individuals, and decides whether it will include that personal data in customer content it stores or processes using the AWS services. The customer may also need to ensure it discloses the purposes for which it collects that data to the relevant data subjects, obtains the data from a permitted source and that it only uses the data for a permitted purpose.

Data Scenario	Summary	Considerations
	information will be collected, used or disclosed. There may be requirements about who personal data may be collected from, i.e. the requirements may differ if personal data is collected from a third party source instead of directly from the individual. Collection of personal data may only be permitted if it is for a valid or reasonable purpose.	As between the customer and AWS, the customer has a relationship with the individuals whose personal data the customer stores on AWS, and therefore the customer is able to communicate directly with them about collection and treatment of their personal data. The customer rather than AWS will also know the scope of any notifications given to, or consents obtained by the customer from, such individuals relating to the collection of their personal data. AWS: AWS does not collect personal data from individuals whose personal data is included in content a customer stores or processes using AWS, and AWS has no contact with them. Therefore, AWS is not required and is unable in the circumstances to communicate with the relevant individuals to seek any required consents. AWS only uses customer content to provide the AWS services selected by each customer to that customer and does not use customer content for any other purposes.
Using and disclosing personal data	It will likely be appropriate or necessary to only use or disclose personal data for the purpose for which it was collected. This may also mean that the individual (data subject) should be informed that the customer will use AWS as a service provider.	Customer: The customer determines and controls why it collects personal data, what it will be used for, who it can be used by and who it is disclosed to. The customer must ensure it only does so for permitted purposes. If the customer chooses to include personal data in customer content stored in AWS, the customer controls the format and structure of its content and how it is protected from disclosure to unauthorized parties including whether it is anonymised or encrypted. The customer will know whether it uses the AWS services to store or process customer content containing personal data, and therefore is best placed to inform individuals that it will use AWS as a service provider, if required. AWS: AWS only uses customer content to provide the AWS services selected by each customer to that customer and does not use customer content for other purposes.
Offshoring personal data	If transferring personal data offshore it may be necessary or appropriate to inform individuals (data subjects) of the countries in which the customer will store their personal data, and/or seek consent to store their personal data in that location. It may also be important to consider the comparable protections afforded by the privacy regime in the relevant country where personal data will reside.	Customer: If a customer has a geographical or regional constraint, the customer can manage this by choosing the AWS Region(s) to align to their requirements, and their content will be stored and processed in their chosen Region(s). The customer should consider whether it should disclose to individuals the locations in which it stores or processes their personal data and obtain any required consents relating to such locations from the relevant individuals if necessary. As between the customer and AWS, the customer has a relationship with the individuals whose personal data the customer stores on AWS, and therefore the customer is able to communicate directly with them about such matters. AWS: AWS only stores and processes customer content in the Region(s), and using the services, each customer chooses, and otherwise will not move customer content, except as legally required. If a customer chooses to store content in more than one Region, or copy or move content between Regions, that is solely the customer's choice, and the customer will continue to maintain effective control of its content, wherever it is stored and processed.

Data Scenario	Summary	Considerations
		General: AWS is ISO 27001 certified and offers robust security features to all customers, regardless of the geographical Region in which they store their content.
Securing personal data	It will be important to take steps to protect the security of personal data.	Customer: Customers are responsible for security in the cloud, including security of their content (and personal data included in their content). AWS: AWS is responsible for managing the security of the underlying cloud environment. For a complete list of all the security measures built into the core AWS cloud infrastructure, platforms, and services, please read our Overview of Security Processes13 whitepaper. Customers can validate the security controls in place within the AWS environment through AWS certifications and reports, including the AWS Service Organization Control (SOC) 1, 2 and 3 reports, ISO 27001, 27017 and 27018 certifications and PCI-DSS compliance reports.
Accessing and correcting personal data	Individuals (data subjects) may need to access their personal data, including for the purposes of correcting it.	Customer: The customer retains control of content stored or processed using AWS, including control over how that content is secured and who can access and amend that content. In addition, as between the customer and AWS, the customer has a relationship with the individuals whose personal data is included in customer content stored or processed using AWS services. The customer rather than AWS is therefore able to work with relevant individuals to provide them access to, and the ability to correct, personal data included in customer content. AWS: AWS only uses customer content to provide the AWS services selected by each customer to that customer, and AWS has no contact with the individuals whose personal data is included in content a customer stores or processes using the AWS services. Given this, and the level of control customers enjoy over customer content, AWS is not required, and is unable in the circumstances, to provide such individuals with access to, or the ability to correct, their personal data.
Maintaining the quality of personal data	It may be important to ensure that personal data is accurate, and that integrity of that personal data is maintained.	Customer: When a customer chooses to store or process content containing personal data using AWS, the customer has control over the quality of that content and the customer retains access to and can correct it. This means that the customer must take all required steps to ensure that personal data included in customer content is accurate, complete, not misleading and kept up-to-date. AWS: AWS's SOC 1, Type 2 report includes controls that provide reasonable assurance that data integrity is maintained through all phases including transmission, storage and processing.
Deleting or deidentifying personal data	Personal data typically should not be kept for longer than is reasonably required for the purposes for which the data was collected and otherwise should typically only be retained in accordance with relevant data retention laws.	Customer: Only the customer knows why personal data included in customer content stored on AWS was collected, and only the customer knows when it is no longer necessary to retain that personal data for legitimate purposes. The customer should delete or anonymize the personal data when no longer needed. AWS: The AWS services provide the customer with controls to enable the customer to delete content, as described in the documentation available at: http://aws.amazon.com/documentation.

Data Classification

Another method of assessing the guidelines around the movement, management, and governance of data, especially across borders, would be to know what *type* of data is in question. Classifying data into discrete categories enables better-informed decisions to be made with regard to access, storing and transmission of data. Data classifications achieve stronger outcomes for organizations by clarifying the safeguards required for different types of data, thereby reducing uncertainty, standardizing access, and reducing costs. It also enables business and other organizations to be able to better use and manage appropriately classified data.

A potential simple data classification framework commonly used in the Public Sector divides data into three tiers:

- **Tier 1: non-sensitive or "Unclassified" data,** the lowest level of sensitivity that makes up most data types, data in this category is not considered critical or significantly detrimental to the national interest if disclosed,
- **Tier 2: restricted or semi-sensitive data**, data in this category may require additional assurance or specific controls applied to ensure that it is appropriately protected against a more severe threat scenario, disclosure may be considered detrimental to the national interest.
- **Tier 3: highly confidential data**, this data requires the highest level of assurance and most stringent security controls to protect it from the most severe threat scenarios and most motivated actors, if harmed there may be significant detrimental impact to the national interest .

Based on a CSPs ability to address the requirements defined for a given data classification organizations are recommended to select an appropriate cloud deployment model.

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?

Cloud customers should retain control and ownership over their data and have the ability to choose the geographic location(s) in which to store their data, with CSP identity and access controls available to restrict access to customer infrastructure and data. CSPs should provide customers with a choice as to how they store, manage, and protect their data, where the customer retains control over where the data is being stored so that the cloud customer understands which jurisdiction their data is subject to and the rules by which their data can be accessed – e.g. by government authorities. AWS data centres are built in clusters in various global regions, and cloud users are allowed to choose to use one Region, all Regions or any combination of Regions.

AWS has devoted considerable energy to publicly outline our position on lawful interception, and the below is drawn directly from public AWS blogs on the issue:

- AWS does not disclose customer information unless we're required to do so to comply with a legally valid and binding order. Unless prohibited from doing so or there is clear indication of illegal conduct in connection with the use of AWS products or services, AWS notifies customers before disclosing content information.

- Where we need to act publicly to protect customers, we do. AWS never participated in the NSA's PRISM program. We have repeatedly challenged government subpoenas for customer information that we believed were overbroad, winning decisions that have helped to set the legal standards for protecting customer speech and privacy interests. We also advocate in Congress to modernize outdated privacy laws to require law enforcement to obtain a search warrant from a court to get the content of customer communications. That's the appropriate standard, and it's the standard we follow.
- While we recognize the legitimate needs of law enforcement agencies to investigate criminal and terrorist activity, and cooperate with them when they observe legal safeguards for conducting such investigations, we oppose legislation mandating or prohibiting security or encryption technologies that would have the effect of weakening the security of products, systems, or services our customers use, whether they be individual consumers or business customers. We offer AWS clients strong encryption as one of many standard security features, and we provide them the option to manage their own encryption keys. We publish security best practices documents on our website and encourage our clients to use these measures to protect sensitive content.
- We are certified under the Safe Harbor Framework and are members of numerous associations focused on protecting privacy and security, and AWS has achieved a number of internationally recognized certifications and accreditations demonstrating compliance with third-party assurance frameworks. AWS clients have control over their content and where it resides.[18]

Data Sovereignty

The benefits of cloud are best realized when there are no data residency restrictions placed on data. Data residency restrictions undermine the economies of scale as well as the security benefits to be gained from shared computing infrastructure.

Nevertheless, where organizations have concerns about the application of regulatory jurisdictions to data, then the customer should ensure that they limit their use of Regions to AWS region that maintains jurisdiction by the regulator and appropriate security standards and controls should be employed or the organisation should work with the TRAI.

Queries are often raised about the rights of domestic and foreign government agencies to access content held in cloud services. Customers are often confused about issues of data sovereignty, including whether and in what circumstances governments may have access to their content. The local laws that apply in the jurisdiction where the content is located are an important consideration for some customers. However, customers also need to consider whether laws in other jurisdictions may apply to them. Customers should seek legal advice to understand the application of relevant laws to their business and operations.

Legal Government Access

When concerns or questions are raised about the rights of domestic or foreign governments to seek access to content stored in the cloud, it is important to understand that relevant government bodies may have rights to issue requests for such content under laws that already apply to the customer. Cloud providers should not disclose customer information unless required to do so to comply with a legally valid and

[18] https://blogs.aws.amazon.com/security/blog/tag/Transparency+report

binding order. Unless prohibited from doing so or there is clear indication of illegal conduct in connection with the use of cloud products or services, cloud providers should notify customers before disclosing content information.

For example, a company doing business in Country X could be subject to a legal request for information even if the content is stored in Country Y. Typically, a government agency seeking access to the data of an entity will address any request for information directly to that entity rather than to the cloud provider.

Extraterritorial Requests for Data

Most countries have legislation that enables law enforcement and government security bodies to seek access to information. In fact, most countries have processes (including Mutual Legal Assistance Treaties or MLATs) to enable the transfer of information to other countries in response to appropriate legal requests for information (e.g. relating to criminal acts). **However, it is important to remember that each relevant law will contain criteria that must be satisfied in order for the relevant law enforcement body to make a valid request. For example, the government agency seeking access may need to show it has a valid reason for requiring a party to provide access to content, and may need to obtain a court order or warrant.**

Many countries have data access laws which purport to apply extraterritorially. An example of a U.S. law with extra-territorial reach that is often mentioned in the context of cloud services is the U.S. Patriot Act. The Patriot Act is similar to laws in other developed nations that enable governments to obtain information with respect to investigations relating to international terrorism and other foreign intelligence issues.

Any request for documents under the Patriot Act requires a court order demonstrating that the request complies with the law, including, for example, that the request is related to legitimate investigations. The Patriot Act generally applies to all companies with an operation in the U.S., irrespective of where they are incorporated and/or operating globally and irrespective of whether the information is stored in the cloud, in an on-site data center or in physical records. **This means that companies headquartered or operating outside the United States, which also do business in the United States, may find they are subject to the Patriot Act by reason of their own business operations.**

Granting government access

Cloud providers should be vigilant about customers' security and should not disclose or move data in response to a request from the U.S. or other government unless legally required to do so in order to comply with a legally valid and binding order, such as a subpoena or a court order, or as is otherwise required by applicable law. Additionally, a good practice is to notify customers where practicable before disclosing their content so they can seek protection from disclosure, unless legally prohibited from doing so or there is clear indication of illegal conduct in connection with the use of the cloud provider's services.

Common Privacy and Data Protection Considerations

Many countries have laws designed to protect the privacy of personal data. Some countries have one comprehensive data protection law, while others address data protection in a more nuanced way, through a variety of laws and regulations. While legal and regulatory requirements will differ – including due to jurisdictional requirements, industry specific requirements and content-specific requirements - there are some common considerations that arise under several leading data protection laws. These can be aligned to the typical lifecycle of personal data.

To help customers analyse and address their privacy and data protection requirements when using AWS to store and process content containing personal data, we discuss below various stages of this data lifecycle, identify key considerations relevant to each stage, and provide relevant information about how the AWS services operate.

Many data protection laws allocate responsibilities having regard to how a party interacts with personal data, and the level of access and control they have over that personal data. One common approach is to distinguish between a data controller, data processor and data subject. The terminology used in different jurisdictions may vary, and some laws make subtler distinctions. AWS appreciates that its services are used in many different contexts for different business purposes, and that there may be multiple parties involved in the data lifecycle of personal data included in customer content stored or processed using AWS services. For simplicity, the guidance below assumes that, in the context of customer content stored or processed using the AWS services, the customer:

1. Collects personal data from its end users or other individuals (data subjects), and determines the purpose for which the customer requires and will use the personal data
2. Has the capacity to control who can access, update and use the personal data
3. Manages the relationship with the individual about whom the personal data relates (referred to in this section as a data subject), including by communicating with the data subject as required to comply with any relevant disclosure and consent requirements.

As such, the customer performs a role similar to that of a data controller, as it controls its content and makes decisions about treatment of that content, including who is authorized to process that content on its behalf. By comparison AWS performs a role similar to that of a data processor, as AWS only uses customer content to provide the AWS services selected by each customer to that customer and does not use customer content for other purposes. Note that the terms “data processor” and “data controller” have a very distinct meaning under different jurisdictional law and this submission is not intended to address those specific requirements.

Where a customer processes personal data using the AWS services on behalf of and according to the directions of a third party (who may be the controller of the personal data or another third party with whom it has a business relationship), the customer responsibilities referenced in the table will be shared and managed between the customer and that third party.

Cloud user responsibilities

Depending on the cloud provider, cloud users are subject to Acceptable Use Policies (AUP) or Terms of Service (ToS). By using the cloud service provided, or accessing the AWS Site, the cloud user agrees to this policy. Violating the policy or authorising or helping others to violate the policy might result in suspension or termination of the cloud user, by the cloud provider.

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

Cloud services should be considered a regular business which is registered to conduct business in India, rather than to have additional requirements placed on them, as this may have the impact of slowing cloud development and adoption if overly-onerous requirements are imposed. We are not aware that there is any other jurisdiction which imposes additional requirements (such as licensing) on cloud providers, as business registration and reporting requirements will address the responsibilities of the cloud business, without needing to create a new regulatory and legal framework around cloud computing.

In order to ensure a level of service quality, a recommended approach would be to ensure that there is a baseline level of certification or accreditation around specific concerns, such as network and information security. Because the public sector is still evolving in its maturity and use of cloud computing, the approach which uses market-driven accreditation and standards will ensure the most current standards of quality as decided by the market are implemented.

Third Party Baseline Accreditations

Leveraging industry best practices regarding security, privacy, and auditing provides assurance that effective physical and logical security controls are in place, preventing overly burdensome processes or approval workflows that are not justified by real risk and compliance needs. There are many security frameworks, best practices, audit standards, and standardized controls that cloud solicitations can cite, such as:

- Federal Risk and Authorization Management Program (FedRAMP)
- Service Organization Controls (SOC) 1/Statement on Standards for Attestation Engagements (SSAE) 16/International Standard on Assurance Engagements (ISAE) 3402 (formerly Statement on Auditing Standards [SAS] No. 70)
- SOC 2
- SOC 3
- Payment Card Industry Data Security Standard (PCI DSS)
- International Organization for Standardization (ISO) 27001
- ISO 9001
- Department of Defense Risk Management Framework (DoD RMF, Cloud Security Model)
- Federal Information Security Management Act (FISMA)
- International Traffic in Arms Regulations (ITAR)
- Federal Information Processing Standard (FIPS) 140-2
- and others, such as those listed at aws.amazon.com/compliance

National Accreditation Systems or Pre-Qualified Lists for Government Cloud

There have also be instances where governments have put in place accreditation systems or pre-qualified lists of cloud vendors, specifically for their government cloud marketplaces. These vendors have either passed an accreditations test, and/or have achieved a specific level of security or other requirements, as set out by the government. India has moved down this path with its plan for empanelment of cloud service providers for government services. Some examples of other governments which have done similar empanelment include:

1. New Zealand – Common Capability (CC) contracts establish various supply agreements with approved suppliers for selected common goods or services or works purchased across government. There is a “contracts register” where providers of specific services (such as IT hardware, Mobile voice and data, rental vehicles etc.) are listed online at

http://www.business.govt.nz/procurement/all-of-government-contracts/common-capability-contracts

2. Australia – The Australian Signals Directorate (ASD) has developed an ASD Certified Cloud List, which requires vendors to pass an InfoSec Registered Assessors Program (IRAP) before being allowed to service government contracts. To see the list of certified clouds: http://www.asd.gov.au/infosec/irap/certified_clouds.htm and to see the IRAP process: http://www.asd.gov.au/infosec/irap.htm
3. United Kingdom – The United Kingdom has a G-Cloud Digital Marketplace, where vendors who have applied and qualified are listed on their Digital Marketplace at https://www.digitalmarketplace.service.gov.uk
4. Singapore – The Singapore government has released a Singapore-specific standard for security, called the Multi-Tier Cloud Security (MTCS) Standard, which is detailed here: https://www.ida.gov.sg/Tech-Scene-News/ICT-Standards-and-Framework/MTCS-Certification-Scheme. MTCS seeks to address needs such as transparency of cloud users, as transparency is a way to build trust between CSPs & cloud users. With MTCS, certified CSPs will be able to better spell out the levels of security that they can offer to their users through third-party certification and a self-disclosure requirement for CSPs covering service-oriented information normally captured in Service Level Agreements. The disclosure covers areas including: Data retention; data sovereignty; data portability; liability; availability; BCP/DR; incident and problem management. MTCS SS has three different tiers of security, Tier 1 being the base level and Tier 3 being the most stringent.
    a. Tier 1 – Designed for non-business critical data and system, with baseline security controls to address security risks and threats in potentially low impact information systems using cloud services (e.g.: Web site hosting public information).
    b. Tier 2 – Designed to address the need of most organizations running business critical data and systems through a set of more stringent security controls to address security risks and threats in potentially moderate impact information systems using cloud services to protect business and personal information (e.g.: Confidential business data, email, CRM – customer relation management systems).
    c. Tier 3 – Designed for regulated organizations with specific requirements and more stringent security requirements. Industry specific regulations may be applied in addition to these controls to supplement and address security risks and threats in high impact information systems using cloud services (e.g. highly confidential business data, financial records, medical records).

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?

Data access requests are currently handled under the provisions of the Information Technology Act. One consistent legal framework should be maintained, to ensure that there is consistency in regulations across national and state level government policy.

In cases where there is abuse or suspected abuse by specific AWS users, AWS has provided communication methods where this can be reported and investigated. For example, any abuse of Amazon Elastic Compute Cloud (Amazon EC2) can be reported online at https://aws.amazon.com/forms/report-abuse where it will be investigated.

Cloud providers cannot police content

Cloud service providers cannot police the content and conduct of users on self-service platforms in the same way that intermediaries cannot be responsible for content. The cloud provider is responsible for the resilience of the cloud infrastructure, while the user is responsible for the content, security, and control of data which resides on the cloud.

Cloud providers makes available to each customer the compute, storage, database, networking or other services as described on our website. Customers have a number of options to encrypt their content when using the services, including using AWS encryption features, managing their own encryption keys, or using a third-party encryption mechanism of their own choice.

Cloud providers should not access user data

AWS does not access or use customer content for any purpose other than as legally required and to provide the AWS services selected by each customer, to that customer and its end users. Hence any investigation of a breach of the National security of India should be addressed to the cloud user, as cloud users using AWS maintain and do not release effective control over their content within the AWS environment. The cloud user has control over:

- Where their content will be located, for example the type of storage they use on AWS and the geographic location (by Region) of that storage
- The format, structure and security of their content, including whether it is masked, anonymised or encrypted. AWS offers customers options to implement strong encryption for their customer content in transit or rest, and also provide customers with the option to manage their own encryption keys or use third party encryption mechanisms of their choice
- The administration of access controls, such as identity, access management, permissions and security credentials

This means that cloud users control the entire life-cycle of their content on AWS, and manage their content in accordance with their own specific needs, including content classification, access control, retention and deletion.

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

a. Promoting cloud computing in e-governance projects.

Cloud First Policy

India's Meghraj "Cloud First" policy states "Government departments at the centre and states to first evaluate the option of using the GI Cloud for implementation of all new projects funded by the government. Existing applications, services and projects be evaluated to assess whether they should migrate to the GI Cloud." This policy approach could be implemented more broadly and strictly, with accompanying detail provided to government agencies about appropriate cloud migration

implementation. There is an Indian government policy on Open Source Technology[19] which makes it mandatory for government agencies to use open source technology – the same approach could be taken with a "cloud first" policy for India.

In fact, to many governments such as Singapore, Australia, and New Zealand, cloud computing has brought forth new and more efficient means of managing government information technology resources. The Asia Cloud Computing Association's Cloud Readiness Index 2014 identified this as a key policy driving excellence in rankings – countries with a "Cloud First" policy tended to perform better in cloud readiness.

> *Leading countries all share the ability to arrive at a coherent "cloud first" strategy in both government and business development, to manage the new dimensional demands of data and cloud. Having a cohesive all-of government approach towards gCloud and other public sector cloud initiatives, supporting computerisation efforts of small and medium businesses, ensuring the political will behind broadband rollout continues unabated – these are some examples of how an integrated approach towards cloud computing issues can raise local capacities for the future. (Cloud Readiness Index 2014, Asia Cloud Computing Association.*[20]

India should develop a document which sets out general guiding principles for a "cloud first" approach for government ministries and agencies to consider in adopting cloud computing solutions as a primary part of their information technology planning and procurement. All government-led, government-controlled programmes should be mandated to go "cloud first".

Agency Implementation - All ministries, departments, agencies, government-owned and government-controlled organizations, including educational institutes such as universities and schools and colleges, should be encouraged to adopt cloud computing as the preferred ICT deployment strategy for their own administrative use and delivery of government services. Government agencies should only be allowed to procure non-cloud technology products if there are clear and specific reasons why cloud computing is not a suitable solution.

Shared services – Another way to increase public sector adoption of cloud is for a central government agency to develop shared services for public sector customers, making specific services available to all government agencies. These could also be extended to the private sector such as SMEs to increase their adoption of cloud services.

b. Promoting establishment of data centres in India.

There could be incentives schemes that focus on attracting data centers. Developing incentives that reward large investment in equipment (racks and servers), including imported equipment, similar to the Mega and Ultra Mega programs that incentivize the manufacturing industry. Exemptions or rebates for entry taxes, customs duties, VAT, and GST for imported data center equipment. Develop special economic zones (SEZs), focused on enabling infrastructure for data center builds that provide operational flexibility and reduced compliance. Provide income tax holidays for data centers. Tax incentives should feature in these schemes.

---

[19] Department of Electronics and Information Technology (DeitY), 2014, Policy on Adoption of Open Source Software for Government of India http://deity.gov.in/sites/upload_files/dit/files/policy_on_adoption_of_oss.pdf

[20] http://asiacloudcomputing.org/research/cri2014

Another idea would be to develop specific value propositions or industrial focus zones, for example the gaming community to be developed in Bangalore, or a financial data center zone to be established within Mumbai. Ancillary support services (such as innovation centers and/or financial regulators) to be located nearby to these zones, to better support the industry's development.

More suggestions are listed in Q21.

c. Encouraging business and private organizations to utilize cloud services

A number of countries such as Singapore have found it useful to implement tax incentive schemes for local businesses to use cloud computing.

Another way to improve the publicity around this would be to identify local cloud champions, and embark on a publicity drive promoting cloud computing in general.

The Ministry of Micro Small and Medium Enterprises (MSMEs) and the Ministry of Commerce and Industry could work to develop more capacity in the local community to use cloud, providing financial subsidies for training.

More suggestions are listed in Q21.

d. To boost Digital India and Smart Cities incentive using cloud.

Similar to part (a), a Cloud First policy would assist to boost the development of Digital India and Smart Cities using cloud computing. This could ensure that cloud computing is built into new city developments, instead of being added on later.

One suggestion would be to focus on the 100 cities which have been identified to become Smart Cities in India, and identify a target group of cities to focus efforts on Internet of Things and Transport applications. Having a number of quick wins which become case studies will create a situation where success breeds success, and other cities can quickly follow suit in adopting cloud and implementing cloud-based solutions for their own cities.

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?

There is no necessity for a dedicated cloud for government applications, unless there is a very clear reason for it. In fact, a dedicated cloud for government applications negates a number of cost-benefits of cloud computing's shared resource model where the cloud service provider owns and maintains the network connected hardware required for their cloud services.

A dedicated cloud need not be considered, unless (1) there are specific security requirements which an outsourced cloud vendor is unable to fulfil, or (2) there are technical requirements which an outsourced cloud provider is unable to fulfil.

Dedicated government cloud does not increase security
A separate government cloud does not increase security, either in a single-tenant or multi-tenant environment. Instead, government agencies should decide what kind of architecture they need in order to meet their needs and achieve their objectives. This involves decisions that are related to aspects of quality of service, including requirements for uptime and security and procuring cloud services where the desired quality of service is stipulated in the procurement contract and service level agreement.

It should be noted that AWS operates a region named GovCloud[21], but this is not only for US Government customers, it is shared by commercial customers. The region is to service the specific requirement of being International Traffic in Arms Regulations (ITAR) compliant. Conversely the FedRAMP accredited region[22] which all US public sector customers can use for Federal Information Security Management Act (FISMA) Moderate workloads is for all regions in the continental US. These are not dedicated regions but are available for use by any of our commercial customers across the world.

Goal-driven government cloud deployments
Successful cloud procurement strategies choose the architecture that meets their requirements. They focus on the objectives of going to cloud, and which then dictate the selection of application-level, performance-based requirements. Government cloud deployment models and decisions should not be dependent on the type of cloud selected (i.e. public, private, hybrid etc.), but rather the end-use requirements. Cloud computing removes the burden of taking care of infrastructure management and upkeep for customers, and thus so is the need to include prescriptive requirements that specify what the underlying infrastructure stack should be.

Industry standards drive quality and security of service
Customers should rely on best practices and third-party accreditations for assurance that the CSP can deliver the desired quality of service, as opposed to dictating the use of specific equipment or procedures (e.g.; racks, server types, etc.). By leveraging commercial cloud industry-standards, customers avoid placing unnecessary restrictions on the services they can utilize, and avail access to the most innovative and cost effective cloud infrastructure solutions.

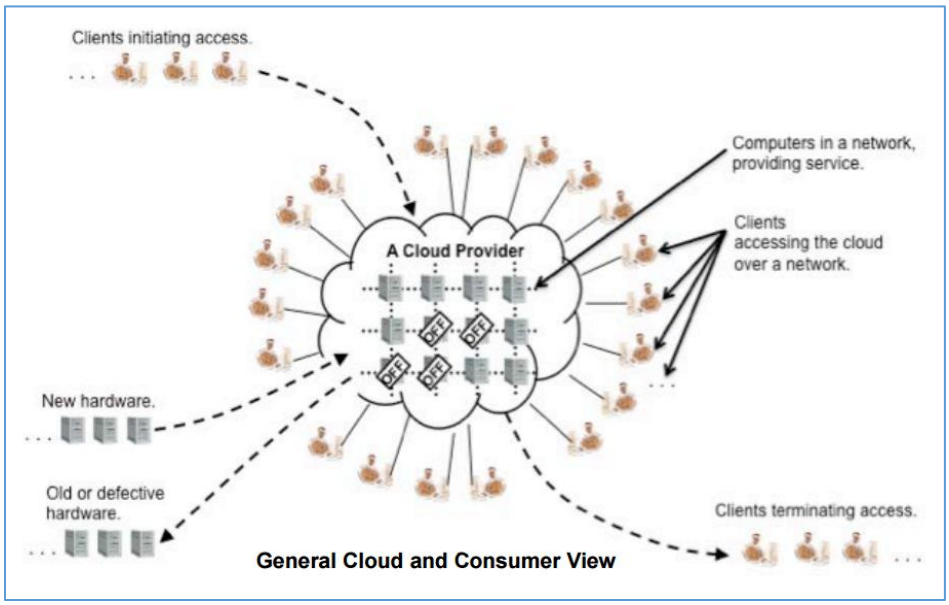
20. What infrastructure challenges does India face towards development and deployment of state data centers in India? What should be the protocol for information sharing between states and between state and central?

INFRASTRUCTURE NEEDED
The development of a robust cloud ecosystem requires that resilient network connectivity on a national and state level. The National Institute of Standards and Technology (NIST)[23] depiction of general cloud environments describes a cloud system as a collection of computing resources the customers can access over a network. They employ a server-side model, which means that customers can send messages over a network to server computers, which then perform work in response to the messages received – see figure below.

[21] https://aws.amazon.com/govcloud-us/faqs/

[22] https://aws.amazon.com/compliance/fedramp/

[23] NIST, 2012, Cloud Computing Synopsis and Recommendations: Recommendations of the National Institute of Standards and Technology http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf



India is in a good position to become a regional hub for Asia's cloud and data centre needs. There are opportunities to build economies of size and scale in the country, and integration with the global value chain is easy with its large English-speaking population.

In recent years, there have also been many opportunities to develop large-scale infrastructure projects – such as data centre builds – at a comparatively lower cost to the region. In addition, while there are challenges that come with the lack of a cross-country electrical grid at the moment, there has been much progress made in electricity and sustainable power development in India, particularly in the Northern states of India.

Other infrastructure challenges center around a range of networking and telecommunication issues, detailed below:

1. *Relaxing rules around access to dark fibre.* There are numerous licenses under which a vendor can lease dark fibre in India, such as IP-I (Infrastructure Provider), UAS (Unified Access Services), NLD (National Long Distance License), ISP (Internet Service Provider) and the latest (which will replace all of the foregoing from 2012 and on), UL (Unified License). These licenses typically have obligations and restrictions on the vendor, and may include restrictions on the types of customers to whom the vendor can lease dark fibre. Because CSP use of connectivity involves use of dark fibre for their internal purposes to connect data centres, it is not expressly addressed by applicable law, and thus many carriers take the conservative view that they cannot lease dark fibre to any person that is not a telecom licensee. *This is a regulatory blocker which should be addressed and removed in order to allow more data centre investors to build and connect data sites in India.*

2. *Develop an open Internet exchange*. We recommend that a truly open exchange model be implemented for all cloud service providers to interconnect, similar to the AMS-IX exchange (in Amsterdam) and other large and successful peering fabrics. Such a model supports more robust and lower cost exchange of data between content providers and Indian customers and end

consumers. A successful exchange will not only make an India investment more attractive to data centre players, but will also bring more local content and allow greater performance.

3. *Allowing and regulating access to telecom or other duct for fibre optic cable, and constructing fibre ducts where none exist* – If a cloud service provider were to build within India and meet with success and increasing demand for their services, they will require additional data centres to be constructed near the initial data centre build. To link these "parent and child" data centres, a cloud provider would use bulk dark fibre, deploying thousands of fibre strands. This bulk fibre reduces the overall cost of data transmission, eliminating costly Dense Wavelength Division Multiplexing (DWDM) equipment and enabling low cost data transmission.

   India should allow cloud providers the ability to license or lease duct or other cable pathways from an Indian Licensed Telecom Operator, or any utility provider and to construct a fibre cable dedicated exclusively for their use between the "parent and child" network nodes and data centre facilities. Duct licenses or leasing rates and terms should be regulated in order to be commensurate with international rates for similar services, eg in Frankfurt, Germany or Dublin, Ireland.

   Where existing telecom duct is not available for lease (because it either does not exist, or the operator has constrained capacity, or specific routing is needed for diversity), new ducts will need to be constructed as part of site development or expansion, utilizing public land to construct a duct or other cable pathway. These ducts will be dedicated exclusively for the cloud provider's use, and built with the appropriate engineering, consultation with the municipality and other utilities, constructed using quality materials and maintained over its life.

4. *Amending rules around network equipment for cloud providers* – there are many equipment used by cloud providers which are similar or identical to telecommunications equipment, such as Ethernet and optical switches, routers and transmission equipment. To encourage data centre development, India could permit the importation and use of network equipment that is used by cloud providers elsewhere in the world, regardless as to that equipment having possible dual-use as telecommunications equipment, provided that the network equipment utilizes a physical medium (copper/fibre) and will not utilize radio spectrum for communications.

Protocol for sharing data between states, and between the state and central government

The more data which can be exchanged securely between states, and between the state and central government, the more efficient a government will be. Different types of data can and should be shared with different protocols. These decisions on data sharing methodologies and protocols should be developed in tandem with a Data Classification regime (see Q14).

A national policy around data sharing on cloud should be discussed and implemented, rather than to have 30 differing state-level policies for data sharing which would be inefficient and undesirable.

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 centers and cloud services platforms in India?

AWS has a good track record of investing in India. In 2016, AWS CEO Jeff Bezos was honoured by the US-India Business Council (USIBC) with a Global Leadership Award, presented by Prime Minister Narendra Modi.[24] We have also committed to invest an additional USD3b in India, boosting AWS total investment to over USD5b.[25]

The economic benefits of such an investment are not simply the injection of foreign direct investment into building data centres and directly providing jobs, but have other knock-on effects and multipliers as well, positively impacting India's output, value-add, and earnings.

There are a multitude of reasons to invest in India, and some favourable considerations for private sector investment include the following:

1. *Tax subsidies to building data centres* – The importance of tax subsidies is important insofar as it helps to keep operational costs down for the cloud provider, who can then pass on the cost savings to customers. Some states have tax incentives for cloud development, which is an incentive that could be deployed on a national level, rather than only limited to the state. These subsidies should be clear and unambiguous, and should not be changed or cancelled with changes in government administrations.

   Consider exemptions or rebates of entry taxes, VAT, customs duties, and GST for data center related equipment (including imported equipment). Ease compliance for existing programs for data centers (i.e., STPI dta requirements).

   Another tax incentive would be tax benefits associated with employing local staff, and exceptions for importing expatriate expertise when so required. Tax exemptions for initial import and setup of data centre equipment would also be an incentive for data centre providers to set up in India.

   Provide tax incentives or grants for educational certifications in the cloud industry to encourage the labour force to become skilled in cloud applications to provide a ready labour force.

2. *Cheaper land and electricity* – Available subsidies and access to land for data center builds would be desirable, as would guaranteed lower electricity tariffs.

   Provide support for infrastructure investment (energy, water, fibre, etc.) by state and local governments to encourage readiness for data center investment.

3. *Creating data center-specific economic zoning and incentives schemes,* as current schemes are often written with manufacturing in mind, and do not lend themselves easily to developing digital services. Consider developing grant programs similar to the Mega and Ultra Mega programs that exist for manufacturing in Maharashtra to encourage large scale investment.

[24] The Indian Express, 8 Jun 2016, PM Modi Presents USIBC Global Leadership Awards To Dilip Shangvhi, Jeff Bezos http://indianexpress.com/videos/news-video/narendra-modi-presents-usibc-global-leadership-awards-to-dilip-shangvhi-jeff-bezos-visit-us-2840766/

[25] The Hindu, 8 Jun 2016, Amazon to increase India investment to $5b http://www.thehindu.com/business/Industry/modi-in-us-amazon-to-increase-india-investment-to-5-billion/article8706252.ece

Consider zoning rules that allow for precertification of sites for data center use to enable the data center to come on line quickly. Provide single point of contact (one stop provider) at the local level to ease the ability to get permits and approvals for data center projects.

4. *Create incentives for managed services to grow as an industry.* India is also the managed service provider to the world, and should seek to maintain its lead in this sector. One incentive to develop the demand for data centres, and also encourage innovation in cloud service platforms, would be to provide tax and other incentives to local companies to develop their managed services capabilities, so that they can use cloud to accelerate their global reach.

5. *Increasing incentives for local cloud demand* - Private sector investment is driven by customer demand, and therefore incentive programmes to increase local appetite and demand for data centre and cloud services should also be put in place. For example, Singapore has a Productivity and Innovation Credit Scheme (PICS) which allows small and medium enterprises (SMEs) to claim tax rebates for using technologies such as cloud computing.[26]

[26] Inland Revenue Authority (IRAS) Singapore Productivity and Innovation Credit Scheme, 7 Jun 2016, https://www.iras.gov.sg/irashome/Schemes/Businesses/Productivity-and-Innovation-Credit-Scheme/