NASSCOM-DSCI Inputs on TRAI Cloud Computing Consultation Paper

NASSCOM®

DSCI
PROMOTING DATA PROTECTION

PREAMBLE

NASSCOM believes that a uniform cloud adoption policy in the nation at all levels, across the centre and states and the broader industry, has the potential to revolutionize India and accelerate the pace of digital transformation, India has embarked upon.

The "cloud" refers to the ICT infrastructure, processing, storage, networks, operating systems and applications that are available *on demand* in variable quantities. It is a boon for small and medium enterprises (SMEs) as well as entrepreneurs that have always faced a challenge of deploying IT infrastructure due to high upfront Capital Expenditure. The pay-for use model that forms an integral part of the cloud ecosystem reduces the IT infra spends by these companies while providing them access to state of the art services ranging from disaster recovery, automatic software updates to providing flexibility of working from anywhere.

Operational agility is the hallmark feature of cloud computing that caters to the ever changing needs of ICT dominated businesses in terms of network bandwidth, scalability and operating costs.

Interoperability is an important aspect in cloud computing and with the shift in paradigm towards a cloud based service delivery model by various organisations there has been a sudden surge in demand of open interfaces and data formats that helps the users retain agility and efficiently transfer data.

However, when we are dealing with cloud based service delivery, given the global reach and spread of the business, it is suggested that the regulations so framed, may have a light touch and be cognizant of what aspects can be regulated in the country.

To the extent possible, for such reasons, how this can be done consistent with prevalent global standards should be considered.

Further, there is also a need to harmonize DeitY cloud policies under IT Act and the TRAI recommendations/directions under the Telegraph Act, as we move forward, and this is an important aspect which we would like to be considered.

The detailed response to specific questions, follows.

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

a. Accelerating the design and roll out of services

Cloud services deliver compute, storage, software, applications, etc. via Internet to customers on a self-serve basis. Customers can subscribe to these services based on their requirements.

NASSCOM believes that these services are flexible, adaptable, and utility based where customers pay for their subscription. On-demand computing resources allows the cloud user to utilise the amount of ICT infrastructure without considering for budgeting, procurement, instalment, configuration and testing.

Enabling the cloud services have several advantages in terms of improved IT efficiency and economies to reduce IT costs. With the pay per usage and Pay As You Go (PAYG) features available in the cloud computing model there is a shift from fixed IT costs to variable costs and further helps in improving the agility and dexterity of government services. The lack of on-premises infrastructure also removes their associated operational costs in the form of power, air conditioning and administration costs and priority is assigned to effective design and roll out of services.

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

India is a nation with ever growing internet penetration and social networking and e-commerce has gradually formed as a backbone of inclusive governance to outreach to the citizens and provide several services that were earlier uneconomical.

Scalability within seconds alongside reliability is the most important requirement for an effective social networking and e-commerce platform to tide over the sudden spikes for information required at critical times.

NASSCOM believes a cloud based platform is the most appropriate platform to meet these requirements. 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. Various collaborative tools can be easily integrated in a cloud based platform without major issues on interoperability and interfacing as compared to the legacy systems.

c. Expansion of new services

The computing middleware which is the prime requirement during augmenting is catered by a service layer in cloud computing: Platform as a Service (PaaS). Herein, the consumers develop their applications and software using a set of programming languages and tools that are supported and provided by the PaaS provider. PaaS provides developers with a high level of abstraction that allows them to focus on developing their applications.

NASSCOM believes developers can provide their customers with a custom developed application without the hassle of defining and maintaining the infrastructure. Therefore, the challenge of procuring the access to enterprise-grade tools is taken care by the cloud architecture. On the other hand, Infrastructure as a Service (IaaS) providers allow their customers access to different kinds of infrastructure (e.g. CPU power, memory and storage) and use the resources to deploy and run their applications through the use of virtual machines which automatically can scale up and down. IaaS therefore provides users flexibility to deploy any software stack on top of the operating system.

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

NASSCOM believes cloud services enhances the accessibility of data and inter-agency collaboration. Information can be shared across verticals, departments with greater efficiency allowing transparency and creativity in delivering public services. Issues regarding data storage, management, and backups, data retrieval are dealt with cloud computing in an easier and cost effective manner.

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

NASSCOM believes that the practicalities of cloud computing will address to the high utilization and smoothing of the inevitable peaks and troughs in workloads. The Cost per unit, project, or product therefore plummets. This enables businesses to better streamline their processes. The workloads will share server infrastructure with other organizations' computing needs. This allows the cloud-computing provider to optimize the hardware needs of its data centres thereby reducing the IT infrastructure costs. The inevitable resultant is lesser power consumption and lower people costs along with zero capital costs to own and run the servers. Cloud enables faster delivery of services and can help improve the agility and dexterity of government services. In addition, its scalability allows agencies to respond to peaks in demand for services.

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

The priorities and the nature of business is the prime determining factor on selection of the cloud service provider by an organisation. NASSCOM believes that there are various factors that are evaluated by an organisation in terms of the perceived benefits, budget vis-a-vis the pricing structure of the cloud service provider (CSP), expertise of the CSP, reliability, flexibility and the scalability of operations. It is the nature of business of the organisation that will determine the choice of a public, private or a hybrid model of the cloud as security and data privacy is also a key aspect in arriving at the decision.

In case of large organisations cost may not be the sole deciding factor in selection of the CSP wherein the focus is on compute-optimized, memory optimized, or storage-optimized services. However, in case of SMEs the decision may be primarily taken from a pricing standpoint. The type of cloud service deployment model by business enterprises are driven by whether the organization can deploy workloads onto public cloud or is it a regulated organization that doesn't allow data/workloads to be deployed onto public cloud.

Since not all processes or data need to be in the cloud therefore the decision on selection of the cloud service provider model is an organisational prerogative and may not be a matter of the regulatory framework.

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

In a competitive operating environment, market forces should be allowed to address interoperability, data portability, migration etc. issues. Migration can be intra-CSP (for example to a different location) or inter CSP (from one CSP to another). For intra CSP migration, CSP and customer will have an agreement that governs terms of service and SLAs for migration. For inter CSP migration, **Cloud service providers will tend to facilitate migration** and portability in creative and innovative ways **without regulatory intervention**, because every CSP has a business interest to attract customers from their competitors and will make available tools to facilitate migration. Unless the incumbent provider does not "lock in" the data by technical means which defeat or block the competitor's migration tools, portability would generally not be an issue. In some scenarios, migration can be as easy as rerouting email traffic from one gateway to another by changing MX record (IP address) of email host server.

CSP gives appropriate security assurances and commits to predefined service levels that will be relevant and sufficient to safeguard the information of everything, depending on the type and volume of data and processes to migrate. The industry is working on developing standards and technology solutions to address these issues e.g. ISO/IEC 19941 standard on 'cloud computing interoperability and portability'.

It is highly desirable for cloud services consumers to have a migration roadmap. A robust migration strategy/ roadmap can help organizations migrate their cloud portfolio from one service provider to another in a secure manner. Certain key aspects could be important: evaluate the interoperability and portability of cloud resources/services that organization is willing to migrate; evaluate the CSP from the vendor lock-in perspective; evaluate security risks and deploy appropriate techniques for example in case of data being migrated from private to public cloud; security of data during migration (to ensure the availability and reduce the risk of data loss); security of applications hosted on the cloud etc. Migrating the data in encrypted form (with state of the art encryption technique) is a good practice. Once migration is successful, the former cloud service provider should destroy the data it holds of customer subject to regulatory requirement of data retention, and as agreed upon in the contractual agreement of cloud service provider.

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

Data control and ownership can become a bit tricky, especially with complex business models around data processing evolving. Data processing can generate further content, which can raise complexity around data control. Meta data is generated around content usage, and further meta-data can be generated around access and use of meta-data. Different models will have different level of responsibility of CSP and customers and both parties, depending on the cloud deployment model chosen, should be clear as to their responsibilities in each model and data ownership. Using a 'one size fits all approach', defining allocation of control and responsibility 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.

If the ownership is clearly established, the customer should be able to retain control and ownership of content owned by it and shall have the ability to exercise full control over movement of data, and demand erasure from the cloud as and when required. CSPs should not access or use customer content except to provide and maintain the cloud services or as legally required, or retain data as per regulatory guidelines.

Data created, collated or derived by the cloud provider in the course of the customers' use of the cloud service, could be usable by CSPs for performing analytics after ensuring de-identification from customer perspective. For example, a cyber security company should be able to retain the data that goes into its threat intelligence that can be used by organization for improving its services, or a CSP should be able to correlate logs to identify security threats.

From B2B or G2B perspective, **data control and ownership should be established using contractual agreement between the parties and there is need for additional provisions** mandating data control specifically for the cloud environment. Regulatory guidelines for privacy will be passed on to Data Processors through Controllers, by way of contractual obligations.

From G2C or B2C perspective, the government has a role to play in providing a clear regulatory environment for data privacy to enable data subject clear access to their personal information stored on Cloud. As per rules issued under sections 43A of Information Technology (Amendment) Act, 2008, Data Controllers processing Sensitive Personal Data or Information ("SPDI" as defined in the Act) have the responsibility of providing Access and Correction facility to Data Subjects for correcting/ updating their SPDI. As ITAA 2008 is limited to SPDI, a much needed comprehensive Privacy Law governing all categories of Personal Information and with horizontal applicability to government and businesses alike is desired.

Question 6. What regulatory framework and standards should be put in

place for ensuring interoperability of cloud services at various levels of implementation viz. abstraction, programming and orchestration layer?

There are various aspects of cloud computing portability and interoperability to consider during the evaluation of the regulatory framework.

The following aspects must be taken into consideration while evaluating the framework for cloud services:

- Enabling re-use of data components across different applications, enabling re-use of application components across cloud PaaS services and traditional computing platforms.
- Ensuring re-use of platform components across cloud IaaS services and non-cloud infrastructure, and interoperability between application components deployed as SaaS.
- And interoperability of the applications using PaaS with applications on platforms using IaaS in a traditional enterprise IT environment.

NASSCOM believes that various international standards such as ISO/IEC 17203:2011 Open Virtualization Format (OVF) specification that are available internationally and are successfully adopted by various countries may be considered as part of the regulatory framework for ensuring cloud interoperability.

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

The cloud computing service is broadly categorized in three segments as Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). All three serve different purposes in different ways to caters to varied business needs therefore the QoS metrics may differ on case to case basis and usually depend on the service level agreement (SLA).

However there are vital QoS model parameters such as network bandwidth variance, virtual machine (VM) startup times, start failure probabilities and other quantifiable QoS attributes such as accountability, agility, assurance of service, cost, performance, security, privacy, and usability that are usually factored in the SLA.

NASSCOM believes that the decision of selection of the CSP may not only be on the above parameters since their exists other non-quantifiable QoS attributes such as service response time, sustainability, suitability, accuracy, transparency, interoperability, availability, reliability and stability which form a critical part of the decision making process while choosing the CSP and drafting the SLA. As a result, there will exist different set of QoS parameters for varied service models including unmanaged cloud services and manged services.

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

Pricing and billing of the cloud services is one of the most complex features and requires in depth understanding into the variety of services availed by the user and the SLA.

NASSCOM believes that the pricing structures are based on a multitude of factors, from storage space needed, clock cycles used, monthly traffic allotments, provisioning of elastic IP, data transfer and load balancing features. The customer should be billed on the basis of agreed pricing models for the usage of the ICT resources. Detailed real time monitoring and metering reports must be made available to the users and alerts can be sent to the customer via appropriate notification channels. The customer must have complete parity in terms of the applications used to assess the demand baseline and usage spikes.

Detailed logs similar to the Call Data Records (CDRs) in telecom can provide the necessary information to address any disputes in billing. Another suggestion is to ensure that billing forms as an integral part of the governance model.

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

Customer complaints and grievances will best be handled by CSP helpdesks or account managers, as this remains a service issue. Metrics for service level and performance are a matter of mutual contract between the cloud provider and its customers and the normal dispute resolution mechanism should be used as and when needed. Disputes that cannot be resolved through this process should be resolved through traditional escalation processes. Greater awareness may be required to enhance transparency, efficiency and predictability in such arrangements.

For Grievance redressal around Privacy concerns related to processing of SPDI by Data Controllers, Rule 5(9) under Section 43A of IT (Amendment) Act, 2008 states that:

"*Body corporate shall address any discrepancies and grievances of their provider of the information with respect to processing of information in a time bound manner. For this purpose, the body corporate shall designate a Grievance Officer and publish his name and contact details on its website. The Grievance Officer shall redress the grievances or provider of information expeditiously but within one month ' from the date of receipt of grievance.*"

Hence, the act already addresses the need and placement of a grievance officer who addresses any discrepancies and grievances of its data subjects (personnel) with respect to processing of SPDI (Sensitive Personal Data or Information) in a time bound manner. For CSPs acting as Data Controllers, they are required to appoint grievance officers and publishing his/her name and contact details on its website and shall be liable to handle grievances within one month from the date of reporting.

However, PI transaction in cloud computing is not only limited to businesses providing services to government or individuals or business customers, but also includes Government to Citizens (G2C) cloud services – example Digital locker service, where government departments or agencies process or store personal information of the individuals. Grievance redressal mechanism should also be built to protect PI which may or may not be SPDI. Since current ITAA 2008 does not guarantee such provision, government should enact comprehensive Privacy bill to give a fillip to Privacy protection and address these privacy concerns arising out of such transactions.

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

Security concerns over cloud can be best addressed through **voluntary adoption of cyber security standards and best practices by CSPs and customers**. The cyber threat landscape is ever evolving and regulatory prescriptions will only drive companies towards compliance instead of addressing such evolving threats.

International Standards for cloud security are already available and many are evolving (ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018 etc.). The customers are increasingly asking CSPs for compliance to such standards.

Competition and brand reputation are significant drivers for CSPs to invest in security. In many cases, the CSPs are able to provide better security than their customers (esp. SMEs & startups) due to focused services. **Ensuring consumer security is in CSP's best interests,** as security is turning out to be important customer considerations. Some organizations are using **security and privacy practices as brand differentiators**.

Data classification and Data Governance framework should be used by the organizations to ascertain the type of security controls to be deployed for classified data. **Attached is the whitepaper prepared by DSCI on the subject,** that will enable organizations to select appropriate cloud services according their need.

Sec 43A rules require Body Corporates (as defined in the rules), including CSPs, to maintain Reasonable Security Practices and Procedures to protect Sensitive Personal Data or Information (as defined in the rules). A well-defined security program, addressing People, Process and Technology aspects and covering all dimensions of security such as technical, managerial, operational, administrative, physical etc., coupled with Privacy Program (often also called as privacy information management system) should be the baseline for all organizations. However the mandate (through regulation or otherwise) should not deeply prescribe the "how to protect" part, rather focus should be on "what to protect" and allow organizations the flexibility to design their security and privacy program suited to their requirements. Mandating the specifics has certain risks such as getting outdated given rapidly evolving technology.

Regulations must not restrict CSPs to deploy state-of-the-art technologies (e.g. limits on encryption), else there is a risk of weakening security.

Cloud providers should also be encouraged to make security as a service available to their customers in a way that can be adapted and tailored to the different needs of each customers. It can be provided as part of the setup or as a value added service on top of the main underlying cloud service.

Question 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.** CSPs should ensure data destruction at exit and should retain data in archival only if there is a legal obligation. From Privacy perspective, regulations can specify the time period for data retention after active processing is complete, or leave it to contractual agreements. Various sectoral regulators have requirements pertaining to data retention for organizations under their purview.

Indian legal framework through section 43A Rule 5(4) has provision for mandating timeframe for retention of SPDI. Section 67C of the IT (Amendment) Act, 2008 data records, logs etc. for intermediaries including TSPs and some content providers, no specific requirements have been detailed through the issuance of rules u/s Sec 43A or 67C. However, various sectoral regulators have issued regulations/guidelines for data retention for organizations under their purview. **Issuing rules under section 43A and 67C at the earliest will help standardize industry practices and expectations on data retention.**

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

Same as question 4

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

This will vary depending on the model of Cloud deployment & relationship between CSPs and customer, and should be left to CSPs and customers to identify mutual roles and responsibilities with respect to security obligations. Various international standards such as ISO 17789 (Cloud computing reference architecture) could be used to derive common expectations around security provisions, and policy should be regularly reviewed.

In case there is any discrepancy between obligation of CSP and end user, it should be resolved through a grievance redressal mechanism. Final resort to adjudicate on the matters will be Court of Law.

Question 14. The law of the user’s country may restrict cross-border

transfer/disclosure of certain information. How can the client be protected in case the Cloud service provider moves data from one jurisdiction to another and a violation takes place? What disclosure guidelines need to be prescribed to avoid such incidents?

Law of the land shall be enforceable on all organizations providing services in India. The legal constraints on ensuring cross border data flow legal compliance should be responsibility of Data Controllers and not Data Processors for data flow between Controller and Processor, and the conditions will be contractually governed, in compliance with law of the land. CSPs acting as Data Processors should process data on behalf of instructions of Data Controllers, including conditions for onward transfer, storing data in a particular geography etc. The CSP as Data Processor may not even be aware of what kind of data the user is putting in the cloud, and what restrictions may apply to a particular type of data. If customer has given specific requirement on disclosure, onward transfers etc., and CSPs violates such contractual arrangements, matter should be resolved between both the parties through legal channel or otherwise. CSPs terms of service should be in compliance with law of land.

For CSPs acting as Data Controllers, they should follow law of the land and are accountable for maintaining compliance to requirements such as disclosure/ onward transfer etc. conditions.

The regulatory requirements and current regime differs from country to country, in case of trans-border data flows and disclosure requirements. Some countries/ regions have strong requirements specific to data being transferred outside the national borders whether in case of outsourced cloud computing services or for processing. For instance, EU Data Protection Directive puts conditions for trans-border data flows, but not specifically for cloud service providers.

Cross border data flows are becoming so fundamental to all business models that they should not be heavily regulated; doing so can impact the digital economy severely. EU uses a heavy handed approach to govern trans-border data flows outside its borders, where it asks for any nation to have "adequacy" status (or laws similar to EU) to protect privacy of EU citizens' and uses Privacy protection as a lever to mandate data localization.

Contrastingly, India does not have such stringent requirements for trans-border data flows. Rule #7 notified under Section 43A of ITAA 2008 says that *transfer of data is allowed only if it is necessary for the performance of the lawful contract between the parties involved and the entity to which SPDI (Sensitive Personal Data or Information) is transferred should be ensured that it has the same level of data protection as is adhered by the transferring body corporate. Also, the data subject is required to be consented before transferring his/her SPDI.*

The conditions for data transfer is business providing adequate data protection, not to maintaining interoperable privacy regime with the country as it does not guarantee protection, but only increases bureaucratic hurdles.

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

The recent ruling of the U.S. Second Circuit Court of Appeals in Microsoft's Ireland email case sends out a strong message to people that they can indeed trust technology as they move their information to the cloud. The Court reversed a ruling ordering Microsoft to turn over emails sought by the DOJ that were stored on a company data centre in Ireland. The case has highlighted ongoing tension between cloud computing providers and governments over data sovereignty and location, and the ruling will likely set precedent over using decades-old laws in the modern era of cloud.

To overcome the challenges of Extra-terrestrial access to data by LEAs, governments including **India should work with the other nations in plurilateral, multilateral and bilateral forums to discuss and come out with practical solutions**. In the age of Internet, global cooperation is quintessential and therefore India should take leadership in identified forums to ensure that its issues are addressed. For example, India should pace up the dialogue on Mutual Legal Assistance Treaty (MLAT) reforms with the U.S. or negotiate a special process for speedy data sharing on crime investigations with the U.S. as presently the Indian LEAs face issues when getting access to data records required from datacenters in the U.S. for investigating crimes that happened in India. India has recently signed a Cyber Fact Sheet with US, and timely access to information and cooperation amongst LEAs is an important consideration in the dialogue between the two nations. Similarly, US Department of Justice is trying to amend its practices so that LEAs of other nation states, can directly get access to data from Organizations established and storing data in the US. India should try and work out such a mechanism with US and other nation states as well.

India should strengthen bilateral, multilaterals, plurilaterals, international treaties and other such mechanisms, and look to improve existing procedures for quick and effective information sharing and getting lawful access to data. **India should reconsider and revaluate Budapest conventions pros and cons, and whether it should result in something meaningful. If India were to become signatory to it.**

Also, Indian LEAs should also be effectively resourced and trained to raise legal requests for gaining lawful access to data from CSPs not located in India through the MLAT route. Further, there is also a dire need to improve procedures and frameworks for data sought by LEAs from CSPs both in India and abroad.

Regarding Lawful interception for data hosted outside India, if it is not done with knowledge of country where data is hosted, it might amount to Surveillance/ Espionage. Hence due legal processes, with precise interpretation of international laws, should be followed by LEAs for obtaining data hosted outside territorial jurisdiction of India.

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

There shall not be any scope to define cloud services in law, coz the model will keep on evolving. Given the relatively early stage of cloud computing development, it is advisable to not resort to regulated approach to structure the cloud computing industry in India. A heavy-handed regulatory approach will likely inhibit growth of the sector. 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. Any kind of licensing or registration goes against the basic mandate of the current government i.e., “ease of doing business” and “liberalize”/“deregulate” what ought not to be regulated.

There are enough regulations in place that are applicable on CSPs, be it ITAA 2008 Reasonable Security Practices and Procedures rules or Intermediary Guidelines etc. If India enacts comprehensive Data Privacy law, CSPs will be under purview of regulation from Data Controller/ Data Processor perspective.

IT-BPM sector boomed in India because there was no specific regulation on the sector. Critical Success factors which led to mushrooming of IT-BPM sector, which contributes to nearly 6% of India’s current GDP, should be replicated for Cloud Services sector. Incentives should be given for establishing Data Centres in India, so that it becomes a significant contributor to our GDP in near future.

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

The multijurisdictional dimension of cloud computing presents a number of legal challenges. The primary concern is about how to balance the needs of law enforcement in an Internet-connected world with the sovereignty of the country. Law of the land should be enforceable on all CSPs who are providing services in India and be subjected to the territorial jurisdiction of India.

CSPs should support Law Enforcement Agencies (LEAs) in crime investigations (access to data records, evidence) and forensics from a Data Controller

perspective. From Data Processor viewpoint, providing services to Government and Businesses, the request for data by LEAs should route through Controllers. Data Processors are not required, nor in a position to, to provide direct access to customer data to LEAs. CSP providing hosting service sometimes are not even aware of what data is hosted by clients. Distinction should be made between Controller and Processor role of CSP and LEAs shall keep in mind the role of the organization while seeking access to information.

The support should be transparent and timely, respecting the laws of the country from where request has originated, respecting the legal requisites based on the location of the data storage. While many of these issues and concerns need global discussions and solutions, the knee-jerk reaction of governments which favours data localization / regulation of content providers is a matter of great concern. **Subjecting CSPs to the requirements of data/infrastructure localization in name of national security will prove to be counterproductive** for variety of reasons including:

- Localization requirements prohibits organizations from achieving economies of scale and leveraging global souring hyper specialization benefits, resulting in increasing cost of services that could be passed on to consumers

- It threaten major new advances in technology and innovation

- It threaten open architecture of the Internet

- If similar policy directions are followed by other countries, it will severely hit established Indian IT-BPM industry sector including the emerging cloud industry which is major contributor to the Indian GDP

CSPs have the responsibility to ensure that all traffic (internet traffic, data, voice etc.) stored with them or flowing their network is adequately protected from external and internal misuse. CSPs should implement well designed Security and Privacy policies, and enforce adequate safeguards and controls to protect data in rest and in motion. They should also maintain well defined access control and usage policy, to ensure data can be accessed only on need-to-know basis. Since cyber security is becoming an integral component of national security, protecting cyber security essential for the organizations. If a CSP is found to be in breach of national security of India as established in the law, proportionate action should be taken against them, as with any other organization.

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

(a) promoting cloud computing in e-governance projects.

NASSCOM believes it is in best interest of the country to implement the “GI Cloud Meghraj” policy for effective eGovernance penetration. Government should mandate all ministries, departments, government owned and controlled organisations, educational institutions etc to adopt cloud computing and imbibe the new paradigm of cloud in their ICT strategy.

(b) promoting establishment of data centres in India

A renewed approach towards the data centre industry will help in establishing a sizeable data centre market in India. NASSCOM believes a variety of steps can be taken to avail this growth opportunity, a separate regulatory policy framework that is transparent and certain in nature only focussing on the data centre market is one of the endeavours that may be undertaken.

Since data centre market is both capital and technologically intensive therefore exemptions, rebate on imports and income tax holidays for data centre can prominently feature as a highlight for schemes to be developed for promoting data centres in India.

A focused approach of creating sector specific data centres such as a FinTech data centre in Mumbai is another way to further promote the data centres.

(c) encouraging business and private organizations utilize cloud services

NASSCOM believes that the cloud services can be promoted by developing programmes and schemes aimed towards incentivising MSMEs using cloud computing and by providing training to the business owners. Offering financial subsides and grants is another way to boost cloud usage amongst organisations.

(d) to boost Digital India and Smart Cities incentive using cloud

NASSCOM believes that by Identifying and awarding the champion cities that have implemented the cloud services and those cities that are using the same to implement the futuristic technologies such as Internet of Things (IoT) and Financial Technologies (FinTech) will provide the much necessary motivation for other cities to follow. A healthy competition between cities may be started to bring about the much needed innovative and disruptive technologies that will arise out of the cloud revolution.

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

As in the case of Meghraj – the government’s own private cloud, there may exist a dedicated cloud for government applications. It is entirely the prerogative of the government to build a dedicated cloud for government applications however, it must be understood that a dedicated cloud may not necessarily increase security.

NASSCOM believes that the decision to go for a public, private or hybrid cloud architecture needs to be taken objectively keeping in view of the end use requirements. Multi-tenancy is a desirable feature because the bigger will be the resource, the higher will be the required number of tenants hence larger would be the economies of scale.

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

India ranks at the bottom of the global pyramid in terms of the infrastructure support available at the federal level to build a data centre due to complicated regulations. The problem is aggravated further due to lack of power and cooling provisions, cost being another major hindrance as any escalation in the energy prices surges the opex of the data centre significantly. There are range of challenges at the centre and state level in terms of availability of physical network and telecommunication issues that cast a dark cloud over the entire data centre ecosystem.

NASSCOM believes that in order to build effective data centres at the state and central levels an open internet exchange must be developed and typecasting of equipment that can used both in telecom and data centre must be dissuaded. It is suggested that importation and use of network equipment used by cloud providers having possible dual-use as telecommunications equipment must be promoted, provided that the network equipment utilizes a physical medium (copper/fibre) and will not utilize radio spectrum for communications.

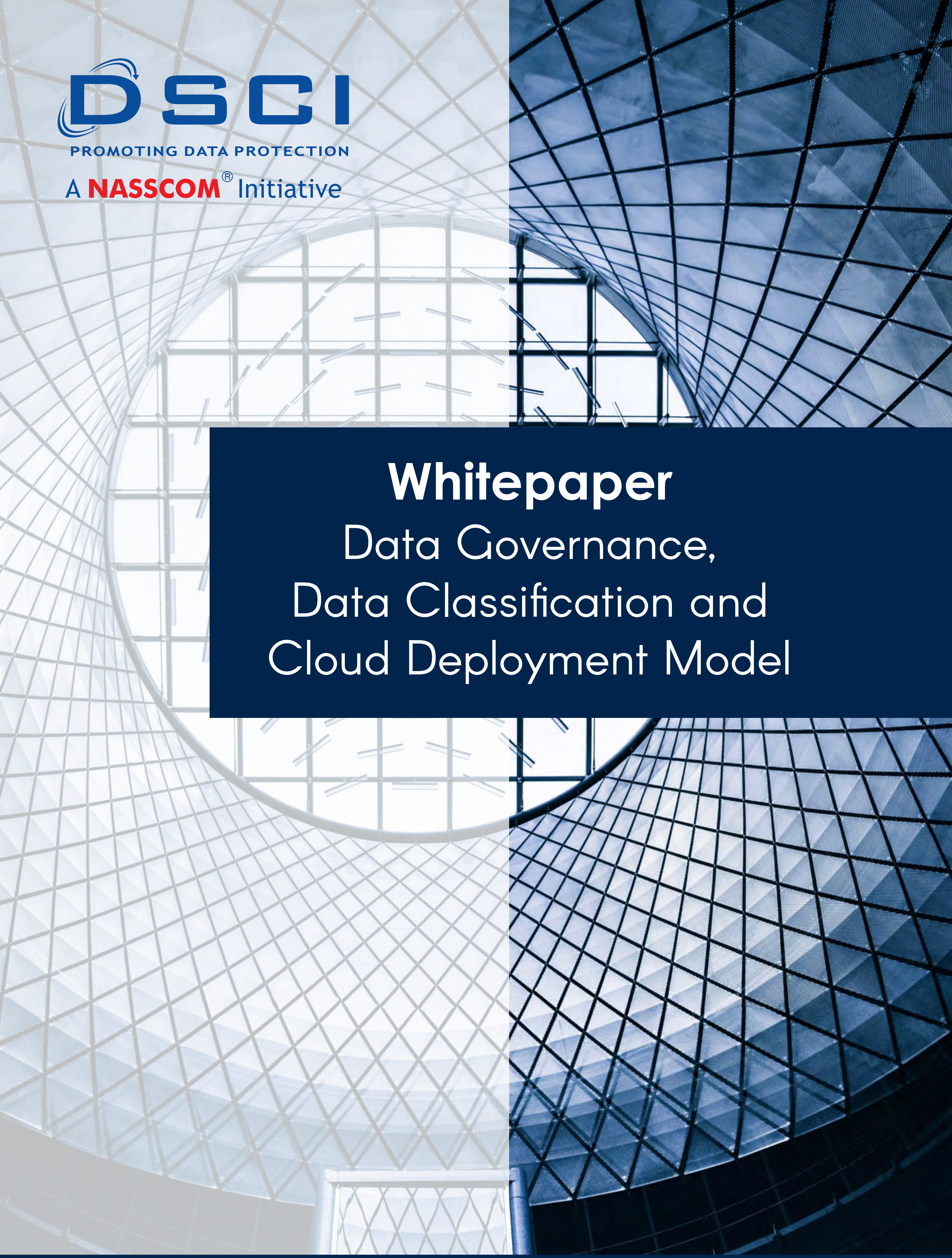
It is therefore not advisable to have differing cloud policy at state levels as various issues emanating from data privacy, security and accessibility standpoint may emerge. Therefore, a policy at the national level after formal consultation and agreement with the various states must be developed and implemented to facilitate data sharing.

Question 21. What tax subsidies should be proposed to incentivise the promotion of Cloud Services in India? Give your comments with justification. What are the other incentives that can be given to private sector for the creation of data centres and cloud services platforms in India?

Financial incentives in the form of tax subsidies to build data centres both at the state and the central level can be provided by the government. Tax incentives for cloud development can consider rebates on VAT, customer duties/GST on data centres. In case of locally deployed resources, income tax exemptions for providing local employment can also serve as a major boost for the industry.

NASSCOM believes that creation of special economic zones with a focus on the Managed Services across the data centre sector can serve as a good motivation to attract investment to harness the full potential of the cloud services. Availability of subsidised land and electricity will also encourage major global players to foray in the

Indian cloud computing market. Policies must be created to enable uninterrupted flow of data across geographies thereby creating a regulatory framework after due diligence that will allow overseas customers to choose India as a destination for their data to be hosted and vice versa. Mutual exchange of information under the lawful vigilance of the regulatory bodies will facilitate and benefit the entire cloud computing ecosystem in India.



DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

Whitepaper

Data Governance, Data Classification and Cloud Deployment Model

May 2016

Data governance (DG) refers to the overall management of the availability, usability, integrity, security and privacy of the data employed in an enterprise. It is an organizational strategy and methodology for documenting and implementing business rules and controls around an organization's data, which may also include personal data of users.

As the IT infrastructure of an organization becomes more open and extends to incorporate various external entities, solutions and interfaces, the exposure surface of the organization expands. Multiple connections to data for multiple usage requirements are increasingly becoming the norms of the day. Cloud computing brings these changes to the IT infrastructure at an astonishingly higher speed and with a surprising ease. Connection to data, its usage and possibilities from it increase multifold. However, it may lead to the questions of integrity, availability, legitimate use, security, and privacy of data being accessed. These questions may pose significant challenges to the organizations migrating to cloud. These challenges demand systematic dealing, setting up of good guiding principles, structural processes, disciplined implementation and organized responses to the eventualities. The concept of Data Governance (DG) emerged from this necessity. Today, it is becoming an integral part of successful cloud migration stories.

Key characteristics of Sound Data Governance Program

(a) A governing body or council tasked with the responsibility of governing data usage in the organization, setting up of guiding principles, polices and rules, overseeing their implementation and ensuring structural response to incidents that might occur

(b) Involving different facets and functions including business, research, solution/product design, corporate functions, HR and legal, apart from technology and operations

(c) A defined set of procedures, and a plan to execute those procedures

(d) Guiding the different parts, functions and processes of taking decisions on various scenarios that might occur around the use of data and taking decisions about underlying infrastructures

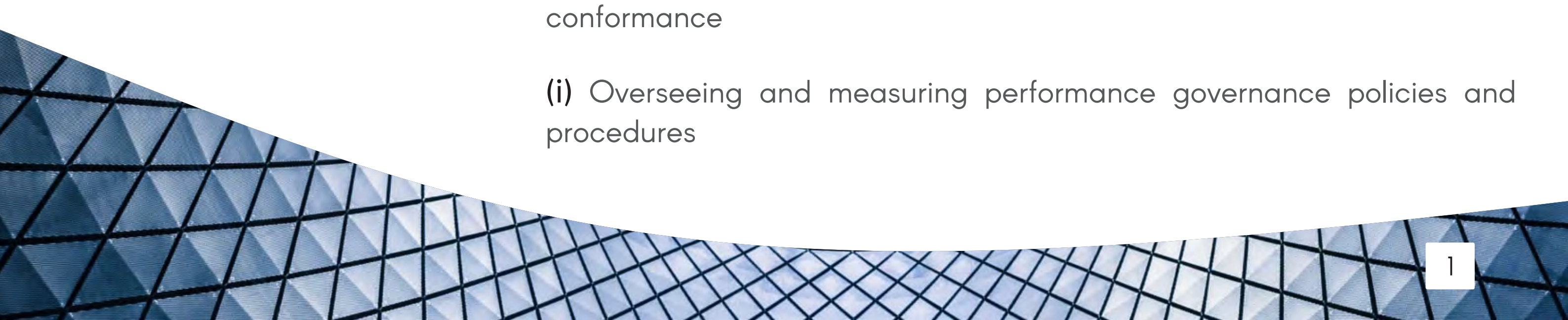
(e) Defining the owners, custodians and users of data assets in the organization. Assisting them with context, scheme and process for identifying, analysing and taking desired actions with respect to the data

(f) Working with the business and IT to develop solutions for critical data issues. Develop sound risk management strategies that can cater to the needs of taking decisions involving data

(g) Bringing up cross-functional teams together to identify data issues that impact the organization as a whole

(h) Setting up effective and efficient processes for identifying legal and regulatory exposures, precisely mapping them to specific steps and arrangement made for compliance and providing assurance over the conformance

(i) Overseeing and measuring performance governance policies and procedures



The initial step in the implementation of a data governance program involves defining the owners or custodians of data assets in the enterprise. A policy that specifies who is accountable for various portions or aspects of the data, including its accuracy, accessibility, consistency, completeness, and updating, must be developed. Processes concerning how the data is to be stored, archived, backed up, and protected from mishaps, theft, or attack, must be defined. A set of standards and procedures must be developed that define how data is to be used by authorized personnel. Finally, a set of controls and audit procedures must be ongoing compliance with government regulations.

Data Classification

A crucial element of an organization's data governance process is Data Classification. Although it has been advocated as a key step in enterprise security program, imperatives of actually taking it for implementation have been getting prominence in the backdrop of transforming IT infrastructure into cloud.

Data Classification involves analyzing, arranging and labelling data elements into predefined, manageable and appropriate data sets or fields.

Benefits of Data Classification

(a) Determine and assign relative values to the data possessed by organizations

(b) Provide means for classification of data based on its level of sensitivity and impact to the organization, should that data be disclosed, altered or destroyed without authorization

(c) Enable business decision making on its usage, transportation, sharing and adoption of different strategies of underlying IT infrastructure including cloud

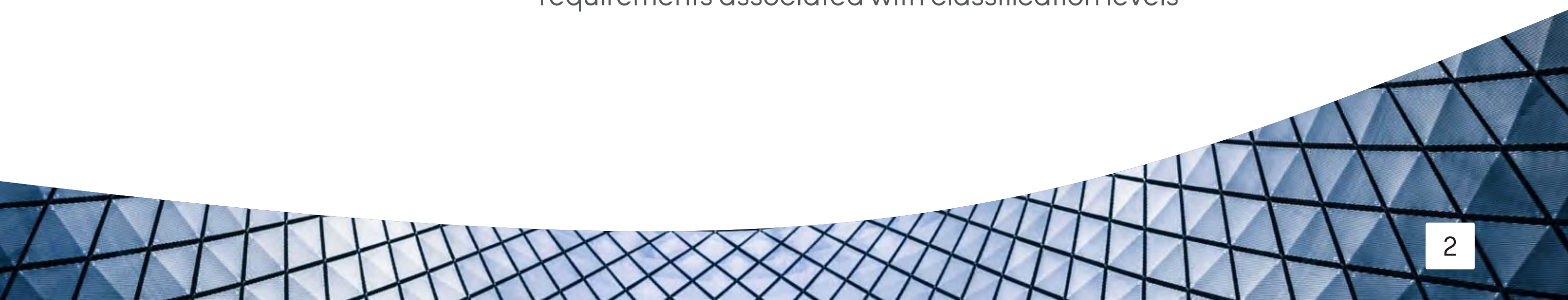
(d) Outline risks and issues that can be mitigated to ensure a smoother transition evolving IT infrastructure building ideas such as cloud computing

(e) Helps in easy search and retrieval of data and use it effectively and efficiently

(f) Enables the separation of data according to data set requirements for various objectives

(g) Helps determine what baseline security controls are appropriate for safeguarding that particular data in a specific classification category

(h) Deploy policies, rules and procedures to fulfil obligations and requirements associated with classification levels



(i) Set up requirements, obligations and assurance norms for responsible and accountable use of data by the extended ecosystem

(j) Oversee and measure conformance to policies, procedures and regulatory compliance associated with classification levels

The issue of data classification rightly falls into a wider set of considerations regarding how organizations should manage their data and overall governance of such data.

Data is a key asset within an organization, yet a number of issues are faced by organizations in the current data-rich cloud environments. One such difficulty is in extracting value from the data – it's almost as if we have more data than what we know what to do with.

Another area, where an organization may have difficulty in managing data, is compliance – new laws, regulations and even basic industry risk considerations are not always well understood. The reality is that these two critical and difficult data management areas can work harmoniously and, if approached correctly, deliver real data value in a compliant manner. Getting these right will offer a positive data value return for organizations.

Data classification is one of the most crucial elements of an effective information governance process—yet it is also one that many companies fail to implement well. In its simplest terms, data classification is the process of categorizing data based on its level of sensitivity. When done properly, the classification of data helps a company determine the most appropriate level of safeguards and controls that need to be in place.

While we don't see this in practice in a lot of cases, data classification fundamentally is the first step to any sort of security or information risk-management program. Organizations don't need to waste time and resources deploying firewalls and other information security controls for data that doesn't need protection, even though they very often do.

Steps towards Data Classification

Steps towards Data Classification

Data classification begins with answering the following questions:

(a) What data, unstructured and structured, does the organization have?

(b) Where does the data reside?

(c) How data is created, accessed and shared in organization's functions, processes and units?

(d) What data is the company trying to protect?

(e) What are the potential risks associated with each data set from a confidentiality, integrity, and availability perspective?

(f) What are the expectations, obligations and liabilities associated with data?

Data Classification, typical categories

Each organization can evolve its own classification scheme. Commonly used classification categories are given as below for reference.

(a) Restricted: Requires the highest level of security controls. Examples include proprietary information and data protected by state or federal privacy rules and regulations

(b) Confidential: Information in which only specific groups of employees are allowed access. Examples include marketing plans, intellectual property, employee lists, and more

(c) Internal use: Information that pertains to employees only. Examples may include employment policies, social media polices, and acceptable use policies

(d) Public: Information with no sensitivity attached to it and will likely result in little or no risk if disclosed, altered, or destroyed—such as press releases

Once sensitive and valuable information has been identified, data stewards should be appointed to oversee the lifecycle of that information. Organizations should be aware that data classification may change throughout the lifecycle. It is important for data stewards to re-evaluate the classification of information on a regular basis, based on changes in regulations and contractual obligations, as well as changes in the use of data or its value to the organization. Data classification is, therefore, a process that needs to have support from the top. This is because data stewards need to be given the authority to make decisions around how to fully implement the data classification program, and also to ensure it is integrated into the company's business practices.

Data Classification in the Indian Government Context

Traditionally, data classification uses the following classification-**Top Secret, Confidential, Restricted and Unclassified.**

(a) This classification is used in government departments and agencies, and appropriate security control are applied based on classified category

(b) Classification is defined in Manual of Departmental Security Instruction, circulated by the Ministry of Home Affairs (MHA) from time to time. MHA last year too.. also published “National Information Security Policy and Guidelines” framework for identifying security controls to be observed

(c) Public Records Act of 1993 also covers certain provisions of handling of data. However, scope and context of applicability of the provisions is not very clear

(d) NIC also issues timely guidelines on security control on be implemented on classified and unclassified data

Cloud Computing

Cloud computing, as per NIST, is defined as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

The increasing need of business, public services, social engagements and personal computing on demand poses significant challenges to on premise applications, services, data and underlying IT infrastructure. The scale of requests seeking access have been increasing multi-fold. The conventional infrastructure struggles to cope with the scale. Infrastructure investment today is likely to get absolute in a short span of time. On premise infrastructure may not have the flexibility and agility to match the fast changing technology world. Investment on it would be unproductive and will prove to be futile in the course of time. Managing inherent legacy systems and ensuring performance and security would be another set of challenges. IT infrastructure needs to be configurable, agile and flexible to imbibe new technology innovation and satisfy scalability requirements. Its management needs to be professional and it should provide high assurance over security. Cloud computing brings these benefits the table.

To determine the best cloud offering, it is important to understand (or at least have a good idea compute, storage, and networking requirements. Requirements of every organization are different and so are its applications, confidentiality, and the level of support required. Cloud deployment models represent the category of cloud environment and are mainly distinguished by the proprietorship, size and access.

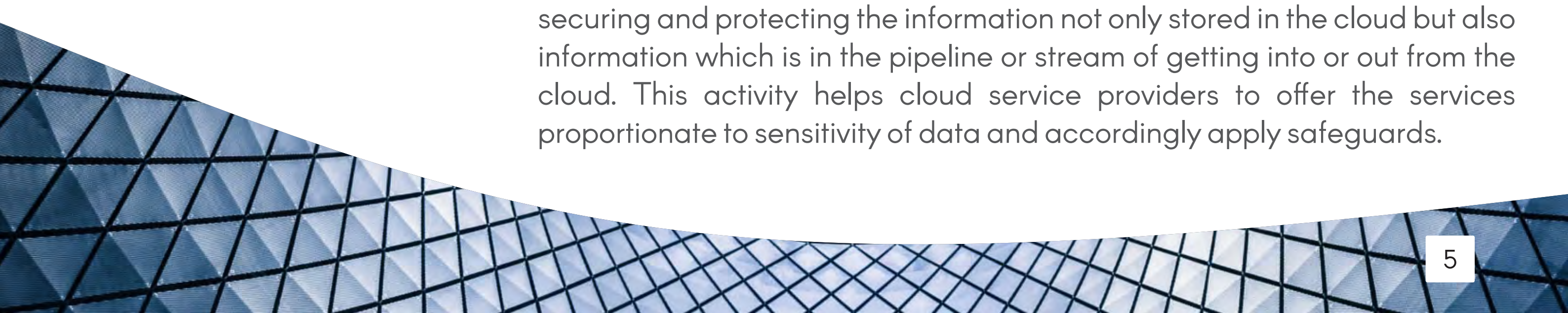
Government of India Cloud (GI Cloud)

For government department and agencies, DeitY has defined cloud deployment in three broad categories namely:

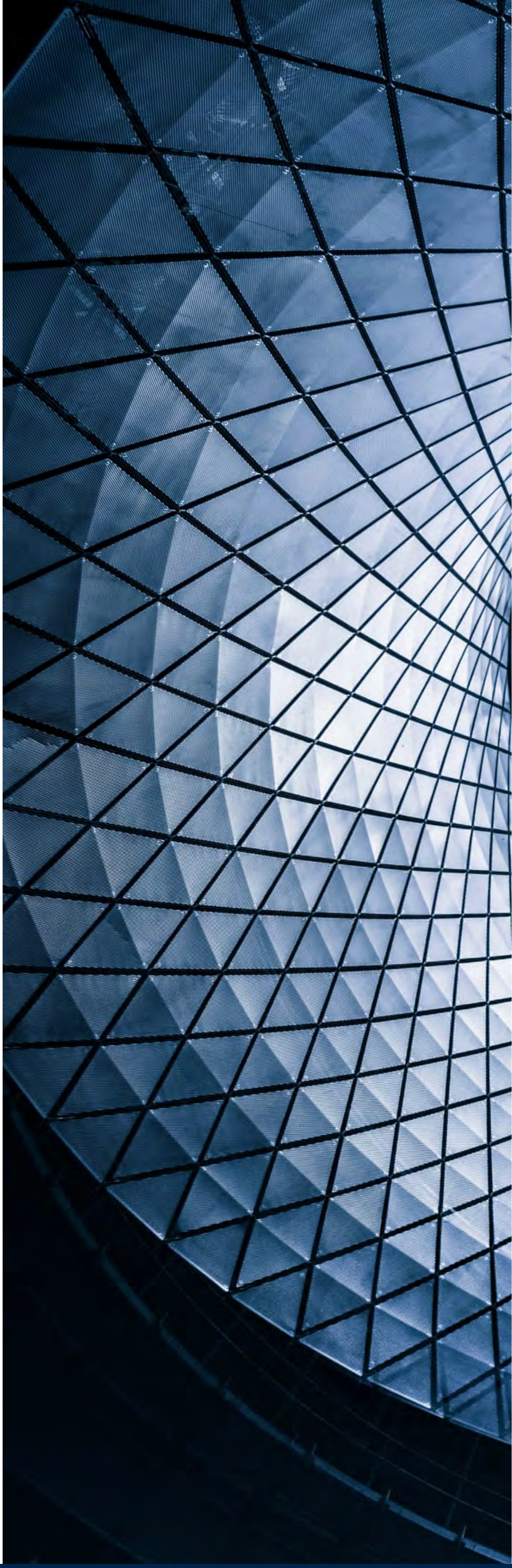
(a) Multi-tenant Public Cloud
(b) Government Community Cloud
(c) Virtual Private Cloud.

Departments often have concerns around risks, security issues, and regulatory compliance associated with cloud computing. On what frameworks and controls be deployed for different categories of data and service is a challenge to solve. What portion of data can be moved to cloud? Shall there be any restriction on cloud adoption for data meant to be in public domain? In the absence of a well-defined framework, organizations find it challenging to also select appropriate cloud services suited to their requirements and needs. A well-informed decision, taking all factors into consideration, will help government organizations choose cloud services between Government Community Cloud, Virtual Private Cloud and Multi-tenant Public Cloud.

When it comes to cloud service providers, implementing critical controls and safeguarding whatever data they store while keeping simplicity at the forefront becomes a mammoth task in the absence of appropriate data classification framework. Data classification plays a very critical role while securing and protecting the information not only stored in the cloud but also information which is in the pipeline or stream of getting into or out from the cloud. This activity helps cloud service providers to offer the services proportionate to sensitivity of data and accordingly apply safeguards.



Therefore a tool (in the form a of Questionnaire) to help organizations select cloud services and how to deploy it becomes useful. The cloud Questionnaire entails all questions that are to be answered by the government department to determine which cloud model it should adopt. The preconceived queries are organized into different buckets as Business, Finance, Legal, Security and Technical. The questions in each category are domain specific and answering a series of questions helps organization to choose the Cloud Computing Model effectively.



Contact us

Niryat Bhawan, 3rd Floor, Rao Tula
Ram Marg, New Delhi - 110057
P: +91-11-26155071 | F: +91-11-26155070
W: www.dsci.in, E: info@dsci.in