Government of India's GI Cloud (Meghraj) Strategic Direction Paper

April 2013

Department of Electronics and Information Technology
Ministry of Communications and Information Technology
Government of India

Acknowledgement

This document has been prepared by Department of Electronics and IT (DeitY) with inputs from the GI Cloud Task Force. We would like to thank all the Task Force members for their valuable suggestions and support. We would also like to thank the PwC Programme Office and others who have directly or indirectly contributed to this report.

In particular, we would like to thank CISCO IBSG, industry associations namely NASSCOM, USIBC and BSA who shared their experiences and provided necessary inputs in finalisation of this document.

Table of Contents

1. Foreword

Cloud computing has the potential to transform the way IT is consumed and managed, resulting in improved cost efficiencies, accelerated innovation, faster time-to-market, and the ability to scale applications on demand.

According to Gartner it is clear that there is a major shift towards the cloud model leading to substantial benefits. The shape of the cloud is emerging, and it is developing rapidly both conceptually as well as in reality. However, the legal, contractual, economic and security aspects of cloud computing are evolving and are yet to attain maturity.

Across the world, governments in the US, the UK, the European Union, Australia and Singapore see cloud services as an opportunity to improve government service delivery outcomes by eliminating redundancy, increasing agility and providing information and communication technology (ICT) services at a cheaper cost.

The Government of India has implemented a number of ICT initiatives under the National e-Governance Plan (NeGP), including creation of ICT infrastructure both at the centre and state levels. The infrastructure thus created will provide the basis for adoption of cloud computing for the government with the objective of making optimum use of existing infrastructure, re-use of applications, efficient service delivery to the citizens and increasing the number of e-transactions in the country, thus helping achieve the ultimate goal of NeGP.

To harness the benefits of cloud, Department of Electronics and IT (DeitY) of Government of India has embarked upon an ambitious project termed as 'GI Cloud'. The 'GI Cloud' is the Government of India's cloud computing environment that will be used by government departments and agencies at the centre and states. In other words, it will enable the government to leverage cloud computing for effective delivery of e-services.

This initiative will comprise the formation and implementation of a cloud computing environment at a national level that will act as a common repository of cloud-based infrastructure resources and applications available on a sharable basis. This will be possible by creating seamlessly operated infrastructure across the country by inter-connecting the components of network and data centres while comprehensively

addressing all security related aspects. This will, inter-alia, enable Rapid Replication of the successfully implemented applications across the country.

While the GI Cloud initiative will focus on setting up an eco-system for cloud adoption by the Government, leveraging the existing infrastructure, DeitY has established a Working Group headed by Shri Kris. Gopalakrishnan to recommend an overall Policy framework for cloud services in the country.

2. Purpose of this paper

This paper aims to provide a strategic direction towards establishing and implementing the GI Cloud and an approach for its adoption by the government. The government ICT infrastructure components that are already in place would act as the building blocks for the envisaged GI Cloud. It identifies the potential risks and challenges of GI Cloud, and its key drivers and benefits.

This paper states the Government of India's vision and policy for its adoption of cloud computing. Finally, it provides a high-level adoption approach for establishing and implementing the GI Cloud.

The intended audience for this paper are the government departments at centre and states and industry. This paper is to be used by the government departments and industry to understand the direction of the government towards adoption of cloud and different definitions, models and services being acknowledged by the government.

A 'GI Cloud Adoption and Implementation Roadmap' will also be published providing a detailed implementation plan of the GI Cloud initiative.

3. The need for GI Cloud

The National e-Governance Plan (NeGP) has led to the creation of common ICT infrastructure such as State Wide Area Networks (SWANs), State Data Centres (SDCs) and Common Service Centres (CSCs) as well as development of guidelines and standards to ensure interoperability, standardisation and integration of various services to provide a single face of the government to the people. The progress of NeGP and other national initiatives like National Data Centres (NDCs), NICNET, National Knowledge Network (NKN) and National Optical Fibre Network (NoFN) highlight the fact that core ICT infrastructure has been rolled out and there is considerable reach in terms of connectivity both at the national and state level.

The GI Cloud is envisaged to be established initially on national and state data centre assets (adapted for the cloud through virtualisation) and connected through existing network infrastructure such as the SWANs, NKN, as well as the internet. Based on demand assessment and taking into account security related considerations, government may also engage the services of private cloud providers.

The GI Cloud will provide services to government departments, citizens and businesses through internet as well as mobile connectivity. In addition to accelerating the delivery of e-services to citizens and businesses , the government's cloud-based service delivery platform will also support a number of other objectives including increased standardisation, interoperability and integration, a move towards an opex model, the pooling of scarce, under-utilised resources and the spread of best practices. It will also support on-going cost effectiveness and manageability.

With cloud computing there is considerable scope of speeding up the development and roll out of e-Governance applications, enhancing agility in customising and deploying ICT to meet specific business needs, while at the same time increasing government ICT efficiency (through re-use and economies of scale).

For realizing this vision and to establish the envisaged cloud computing platform, a well-defined adoption strategy and roadmap are critical.

4. Definition of cloud computing adopted for GI Cloud

The US National Institute of Standards and Technology's (NIST) definition of cloud computing is the most widely adopted one and has been adopted by the Government of India for GI Cloud.

It states the following:

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

The model defined above comprises of five essential characteristics (viz. on-demand self service, ubiquitous network access, metered use, elasticity and resource pooling), three service models (infrastructure as a service, platform as a service and software as a service), and four deployment models (public cloud, private cloud, community cloud and hybrid cloud). These have been depicted in the figure below.

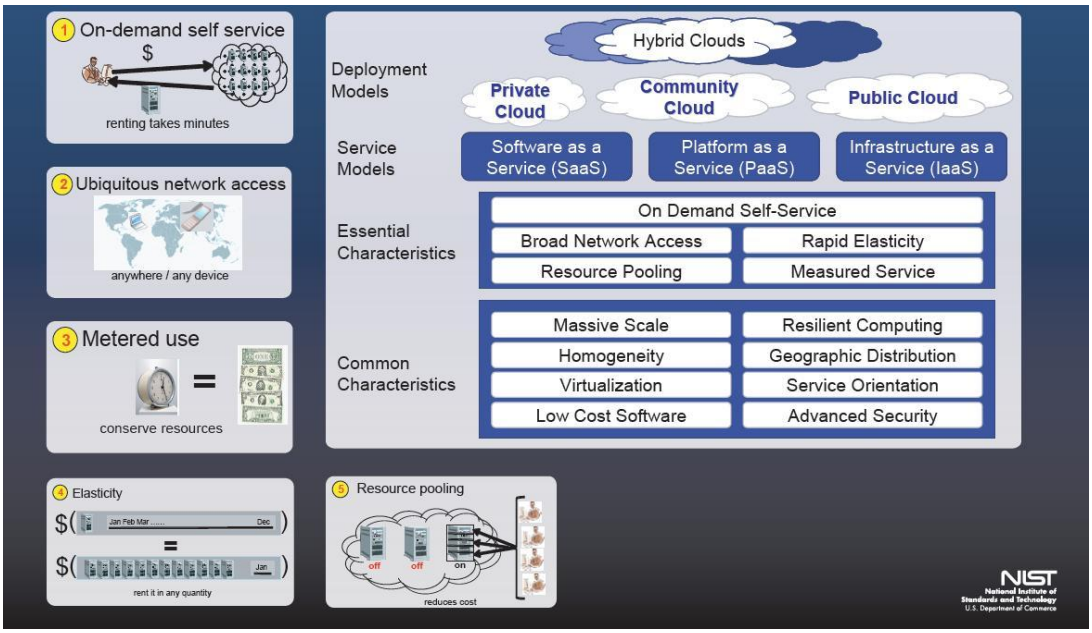

Figure 1: Visual model of NIST Working Definition of Cloud Computing

The definitions of the essential characteristics, service models and deployment models as outlined by NIST have been presented in Annexure III.

5. Key drivers and potential benefits of GI Cloud

- **Optimum utilisation of existing infrastructure:** The government has already invested in core ICT infrastructure build-up. The GI Cloud can initially be built on the existing infrastructure, or by its augmentation. Cloud computing will enable optimum utilisation of this infrastructure and reduce duplication of cost and effort.
- **Rapid deployment and reusability:** Applications developed by one entity (for e.g. departments at the centre and states and private organisations) can be made available on the e-Gov AppStore. These applications can be deployed and re-used by other departments with the required customisations. As a result government departments will have the freedom to focus on their core objectives including policy, programs and process improvements or new applications development where a similar application does not already exist.
- **Manageability and maintainability:** The GI Cloud will provide a single directory of services providing integrated visibility and control helping departments to dispense with the requirement of lengthy procurement and maintenance of ICT infrastructure, an exercise which many find difficult to perform.
- **Scalability:** Applications and infrastructure deployed on the common GI Cloud platform can take advantage of the virtualised nature of the cloud to scale as required. This essentially becomes more useful for applications where there is a burst of demand for ICT resources at regular intervals.
- **Efficient service delivery and agility:** Faced with the continued budget challenges all government departments need to find ways to deliver their services to citizens and business as economically as possible without compromising the achievement of desired outcomes. GI Cloud shall provide the framework for government department at the centre and in states to enable roll out of such services much faster compared to current the traditional mode. Easy and quick access to ICT resources will lead to a faster and more agile service delivery of citizen-centric services by the government.
- **Security:** A security framework for the entire GI Cloud will lead to less environmental complexity and less potential vulnerability. This will also help

bring out the essential interoperability across various cloud environments in the country.

- **Cost reduction:** The pay-per-use model of pricing in cloud will ensure that ICT resources and applications are made available without significant investment in infrastructure purchase and maintenance.
- **Ease of first time IT solution deployment:** Ease of procurement of software as a service provides an opportunity to agencies going for first time automation to leapfrog as they can buy services directly without going through the entire IT evolution cycle.
- **Reduced effort in managing technology:** Since most cloud offerings are based on prebuilt standardised foundation of technology that facilitates better support, GI Cloud will reduce government's effort in managing technology. Easy provisioning of computing resources will ensure more consistent technology upgrades and expedite fulfilment of IT resource requests.
- **Increased user mobility:** Cloud will facilitate user mobility and collaboration through shared data and applications stored in the cloud when authorised – anytime, anywhere availability.
- **Standardisation:** There are outstanding issues that are being faced and dealt by all government departments in order to maintain the reliability, portability, security, privacy, and citizen-confidence & trust in government services. GI Cloud shall prescribe the standards around interoperability, integration, security, data security and portability etc. GI Cloud shall consist of framework for citizen services to comply with standard practices, eliminate vendor lock-in scenarios, etc.

6. Potential risks and issues of GI Cloud

Cloud computing is not a new technology. Rather it is a new model of IT service delivery. As outlined in Gartner's Hype Cycle for Cloud Computing 2012 (refer Annexure II), most cloud computing technologies and concepts are more than two years from mainstream adoption. This signifies the fact that cloud computing is yet to mature both in terms of technology and business readiness as well as adoption by the market. Issues like standards for security, interoperability, licensing, governance and contracting in cloud are still being deliberated upon and work is in progress worldwide. So, a clear understanding of the associated risks is required for the adoption of cloud computing by the government.

Risks and issues	
Cloud standards	• Existing cloud standards pertaining to implementation, storage and migration need to be interpreted to understand their applicability for the GI Cloud environment. • Adoption of open standards as per Government of India's policy on open standards (http://egovstandards.gov.in/) on interoperability and data portability is required in order to reduce the risk of vendor lock-in and inadequate data portability.
Security and privacy	• Risk of compromise of confidential information and intellectual property (IP). • Risk of inappropriate access to personal and confidential information. • Appropriate privacy and security measures need to be in place.
Application design	• Traditional application design approaches are different from cloud based application design. • All new applications must be designed keeping basic cloud design premises in mind. In order to ensure this, guidelines on application development and design need to be adopted. • Existing applications need to be assessed and if required customised in line with cloud design principles to make them cloud ready.

Risks and issues	
Integration with legacy environment	• In order to have a fully operational cloud environment, cloud based applications need to be integrated with existing on-premise legacy applications. • However the opportunity for customisation of existing applications and services may be limited, leading to increased complexity in integrating with existing legacy environments.
Licensing	• Existing software licensing models may not facilitate cloud deployment especially from the point of cloud service delivery. • To facilitate Government departments in deployment of cloud services, a comprehensive framework will be developed on the usage of various licensing models. This framework will be flexible to take into account emerging technologies and business models to leverage the same in the best interest of government.
Location of data	• The dynamic nature of cloud may result in uncertainty as to where data actually resides (or where it is in transit) at a given point in time. This raises concerns related to data ownership, accessibility, privacy and security. • The decision regarding storage and transmittal of data to different cloud models may, therefore, be based on application sensitivity, data classification and other relevant privacy and security related considerations including the regulatory and legal framework of the hosting jurisdiction.
Vendor lock-in	• Due to the rapid emergence of cloud computing through the initiatives of individual companies, many offerings are proprietary in nature, creating challenges in migrating data and applications to the cloud, or switching cloud providers. This puts customers at significant risk if the need arises for systems to interoperate across cloud and in-house environments or to retrieve data and/or applications if a cloud provider withdraws from the market. These issues are to be managed though appropriate standards and contract provisions.
Portability	• Applications developed on one platform may not be portable

Risks and issues	
	to, or executable on another.
Loss of control	• Loss of control may lead to resistance to change. As the need to maintain servers and other data centre infrastructure diminishes, the form of the IT function in government may change. • Users may spawn instances unnecessarily and wastefully, just because it is possible and easy.
Funding model	• Due to the different funding models like pay-per-use , subscription etc. , some part of ICT capital budgeting will need to be translated into operating expenses (OPEX), as opposed to capital expenditure (CAPEX). This will affect budgeting for ICT and may have an effect on the ICT procurement. • New procurement guidelines, funding and a sustainability model need to be identified to address this.
Performance and conformance	• Need to ensure that guaranteed service levels are achieved in the GI Cloud else it may affect effective service delivery. • SLAs are required to be defined for each of the services that will be provided by the GI Cloud. Existing contractual agreements and SLAs both with third part data centre operators, and cloud service providers, may be evaluated and customised to meet the government's requirements • For failure to adhere to the service levels, proper penalty clauses must be incorporated. This will require proper interpretation of SLAs. Proper institutional mechanism should be established to resolve any conflict and provide for timely intervention (if required). • A fully functional 24x7 helpdesk may be incorporated.
Skills requirement	• A direct result of transitioning to a cloud environment results in demand of resources with different skill sets than those in the traditional environment. • Given that the Government departments are generally under-staffed in ICT, this presents an opportunity for requirements identification. A well defined capacity and capability building exercise needs to be carried out across the country to ensure projects do not suffer due to lack of skilled resources

Risks and issues	
	• Ongoing training programmes and plans need to be in place for training existing resources and upgrading their skill set in line with the new requirement
Change management	• More than being a technology, cloud is a new model of service delivery • Adopting cloud across various government departments and agencies at centre and states would call for intensive change management initiatives. The capacity and capability building exercise should incorporate orientation programmes to address these • The procurement teams in state and central nodal agencies need to be trained on procuring for cloud and move away from the traditional experience of procuring hardware and software • Such a comprehensive change management initiative would require proper communication at all levels

7. Vision

To accelerate delivery of e-services provided by the government and to optimise ICT spending of the government.

8. Policy

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.

Policy principles:

- All government clouds to follow the standards and guidelines set by Government of India
- At the time of conceptualisation of any new Mission Mode Project (MMP) or other government project the existing services (IaaS, PaaS, SaaS) of GI Cloud to be evaluated first for usage
- All new applications to be cloud ready

9. Objective

Government of India's objectives in adopting a cloud computing strategy is as follows:

- Optimum utilisation of infrastructure
- Speeding up the development and deployment of eGov applications
- Easy replication of successful applications across States to avoid duplication of effort and cost in development of similar applications
- Availability of certified applications following common standards at one place

10. GI Cloud Strategy

Architectural vision of GI Cloud

The architectural vision of GI Cloud focuses on a set of discrete cloud computing environments spread across multiple locations, built on existing or new (augmented) infrastructure, following a set of common protocols, guidelines and standards issued by the Government of India. The GI Cloud services will be published through a single GI Cloud Services Directory.

The GI Cloud is envisaged to consist of multiple National and State Clouds. The agencies responsible for operating and managing the National and State Clouds may engage Managed Service Providers (MSPs) for managing the respective cloud computing environments.

These cloud computing environments will utilise the existing network infrastructure such as the SWANs, NKN, NOFN integration hubs as well as the internet.

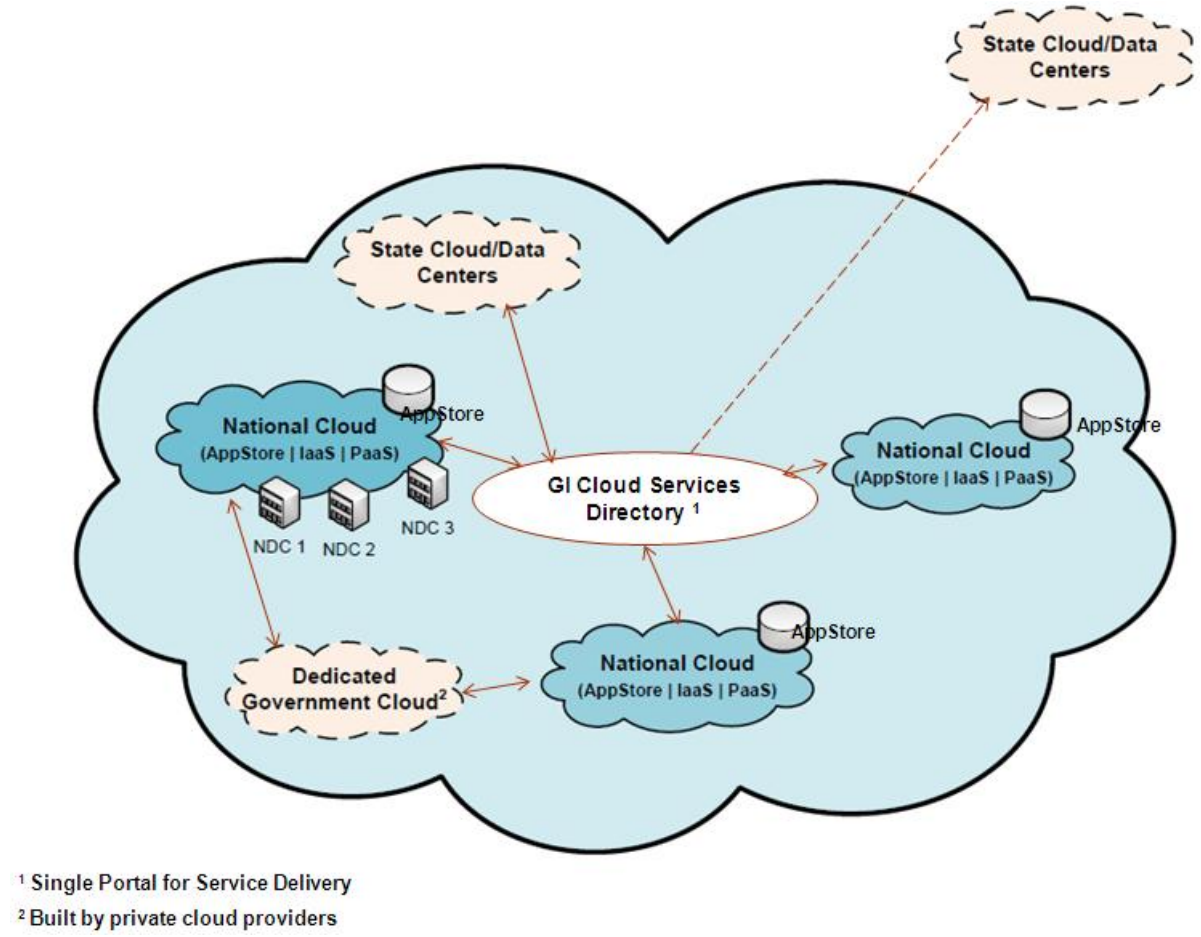

Figure 2: GI Cloud Environment

The figure above depicts an overview of the GI Cloud consisting of cloud computing environments at the national and state levels termed as 'National Clouds' and 'State Clouds' respectively. While one of the National Clouds will be built utilising the infrastructure available under the National Data Centre(s), other National Clouds may also be established. These may be new or established by augmentation of the existing data centres available at state level. Based on demand assessment and taking into account security related considerations, government may also engage the services of private cloud providers. The willing state clouds built on state data centres can also associate themselves with the GI Cloud and publish their services in the GI Cloud Services Directory.

Services provided by National Clouds would include infrastructure (compute, storage and network), platform, backup and recovery, infrastructure scaling of the State Clouds, application development, migration and hosting etc. Over a period of time, other clouds at the national level could also provide remote infrastructure management for the State Clouds.

The vision is also focussed on national and state level shared, reusable applications and services that will allow any government department or agency to accelerate its e-Governance progress by using applications which other agencies or departments have already developed and made available in the government cloud environment. The National Cloud and each of the other clouds at the national level are envisaged to host an 'eGov AppStore' that will act as a common platform to host and run applications at National Clouds which are easily customisable and configurable for reuse by various government agencies/departments at Centre and States without investing effort in development of such applications.

Components of GI Cloud

Deriving from the architectural vision, GI Cloud is envisaged to include the following components:

1. Cloud computing platforms
2. Common platform to host and run applications - eGov AppStore
3. GI Cloud Services Directory that will act as the single window or portal for GI Cloud service delivery
4. Integrated infrastructure acting as a backbone for delivering cloud services
5. Common set of protocols, guidelines and standards for GI Cloud
6. The institutional mechanism will consist of an Empowered Committee and Architecture Management Office. DeitY will be the administrative department responsible for implementation and monitoring of the entire GI Cloud initiative. DeitY will be assisted by Expert Group, CoE, Auditors, Cloud Management Office etc. Agencies responsible to operate cloud environments and provide cloud services
7. Centre of Excellence for cloud computing for awareness building, best practices creation, providing advisory services to the departments on cloud adoption, showcasing the cloud technologies, international collaboration and research and development.

GI Cloud Operations

It is envisaged that the National Clouds may have their own separate operating agencies. These agencies may include a national level government agency or Cloud Utilities.

While the national government agency will be responsible for setting up and operations of a National Cloud, separate Cloud Utilities may be created for setting up and operations of other clouds at the national level. Either existing State Nodal Agencies or National Information Utilities (NIUs) like NSDL, NPCI etc could also be leveraged instead of establishing new Cloud Utilities. A new Cloud Utility may be set up, including a section 25 company. Establishing separate Cloud Utilities for running each of the other clouds at the national level is suggested to ensure competition and better service delivery.

The Cloud Utilities will also provide support services to help the departments in migration and adoption of cloud and development of cloud ready applications as per the policy directions of the government.

GI Cloud Policy – A Mandate

With regard to mandating the use of GI Cloud, it is envisaged that a combination of incentives and sanctions maybe used instead of a pure mandate. A pure mandate does not align interest of stakeholders or establish accountability. The states may not optimally use cloud, and the national government and even cloud providers have little incentive to make the cloud attractive and if it is mandatory. A combination of incentives and sanctions like initial funding for development of cloud ready application, services at subsidised rates etc, can be a highly effective means of efficient, innovative and widespread use of the cloud.

Services to be provided by GI Cloud

Infrastructure-as-a-service (IaaS): The GI Cloud will make available compute, storage and network in an on-demand pay-per-use model to potential departments at centre and states.

Platform-as-a-service: The GI Cloud will make available platforms (programming languages and tools for development and testing of applications that are independent of underlying infrastructure) on-demand. Production environment will also be provided for hosting of applications on the GI Cloud.

Software-as-a-service: Applications (core applications and common applications like payment gateway, messaging platform, MIS reporting etc) can be made available in the GI Cloud through the eGov AppStores or in a pure SaaS model. The eGov AppStores will host both cloud and non-cloud enabled applications. Any department can use the services of eGov AppStores through two primary means – either by directly running the application available from the respective eGov AppStore on a virtualised environment (i.e. used as a service) or can also download the application from the respective eGov AppStore. For complex applications that require major modifications to be used by different states, only a productised version of the same whose core is downloadable will be available at the eGov AppStores. However, for generic applications that can be used by multiple departments at centre and states with little or no modification, options will be provided for running the same from cloud or download from the respective eGov AppStore and run.

Data-as-a-service: GI Cloud will also look at data as a service which is similar to SaaS and the data can be provided on demand to the user.

Though the focus has been on pay-per-use or metered usage model of pricing, other pricing models like flat rate pricing (especially for services that are not usage sensitive e.g. DR) or pricing based on different levels of service/usage bands will be explored and suitably incorporated for GI Cloud.

A GI Cloud Services Directory will be created to provide a single window for discovery of services and related information by the consumer.

Enabling activities for GI Cloud

An Empowered Committee will be formed under the chairmanship of Secretary, DeitY with representations from Central/State line ministries and other government entities. It will provide strategic direction and guidance to DeitY on key matters pertaining to functioning of GI Cloud.

Policies, standards, guidelines and frameworks for GI Cloud will be defined at the national level and will be implemented across the country. While DeitY will be responsible for policy formulation and enforcement, funding, infrastructure enablement and augmentation and other project related approvals, an Architecture Management Office (AMO) and Cloud Management Office (CMO) will be created under DeitY that will define architecture, standard and guidelines for the GI Cloud

and manage day-to-day operations respectively. The standards and guidelines will be developed in consultation with the industry and based on the international best practices. It is proposed to create a 'GI Cloud Expert Group' with experts from the industry to deliberate on these standards/ guidelines.

As Security and Privacy play an important role in the cloud adoption, AMO will also focus on security guidelines defining the various challenges, risks and the approach for mitigating the same. The detailed assessment of application as well as data profiling will also play an important role in terms of understanding the sensitivity of data and its respective challenges that need to be addressed during the development of guidelines.

Capacity and capability building exercise will be carried out across the country both at national and state level for adoption of cloud computing by government. This exercise would also require utilisation of the industry's strengths in this area during the development as well as implementation of the entire program.

Cloud Security

Globally, security considerations remain one of the main factors inhibiting adoption of cloud technology. It is, therefore, imperative to understand and address the risks and challenges associated with adoption of cloud. Usage of cloud should not contribute to increased risks of compromise of confidential information and intellectual property (IP), and inappropriate / unauthorized access to personal information. A robust security framework, therefore, needs to be in place to address such concerns.

GI Cloud Strategy and implementation roadmap reports intend to comprehensively address all the security related aspects. DeitY shall prescribe the standards around interoperability, integration, data security, portability, operational aspects, contract management, etc for the cloud. Architecture Management Office (AMO), an important component of the GI Cloud institutional set up, will be responsible for defining guidelines on security addressing the various challenges, risks and for prescribing the approach for mitigating the risks.

A dedicated security unit will be an essential constituent of the AMO to focus on the standards and guidelines addressing the security concern areas. While evolving the standards and guidelines, the decision regarding storage and transmittal of data to different cloud models may be based on application sensitivity, data classification and other relevant privacy and security related considerations including the regulatory and legal framework of the hosting jurisdiction. The Cloud providers will need to ensure adherence to the prescribed Security Standards and guidelines. The Cloud auditors will also play an important role in ensuring adherence and compliance to the defined guidelines and standards for the complete ecosystem. Capacity building programs will be undertaken to help create the necessary awareness and enhance the knowledge of security related aspects amongst cloud users as well as cloud service providers.

A comprehensive security framework for the entire GI Cloud is thus proposed with the objective to minimise the potential vulnerabilities from adoption of cloud.

Adoption approach

Adoption and establishment of GI Cloud is envisaged in three phases. This has further been elaborated under the section 'Adoption Phases'.

Phase I: Strategy, policy and guidelines establishment

Phase II: Implementation

Phase III: Monitoring, management and ongoing improvement

Adoption phases:

The adoption of GI Cloud is envisaged to be completed in three phases as depicted below:

Phases	Proposed Activities
Phase-I Strategy and policy establishment	a) Establishment of GI Cloud Task Force
	b) Conceptualisation of a government cloud strategy and adoption roadmap, including the following: i. Vision and policy ii. Architecture and implementation roadmap iii. Eco-system and institutional mechanism iv. Business and funding model v. Capacity and capability building plan
	c) Agree on the vision, strategy and conceptual plan and high-level architecture
	d) Define institutional mechanism for GI Cloud
Phase-II Implementation	a) Establish Empowered Committee for GI Cloud
	b) Establish Expert Group for GI Cloud
	c) Set up the National Cloud , National AppStore and Cloud Services Directory by Government Agency
	d) Set up a Centre of Excellence (CoE) including Architecture Management Office (AMO) and Cloud Management Office (CMO) for Cloud Computing
	e) Undertake demand assessment for cloud services with the objective of setting up other cloud environments
	f) Publish GI Cloud standards and guidelines for security, application development and productisation, service delivery, operational aspects etc.
	g) Prepare revised ICT procurement guidelines and contract management practices for GI Cloud
	h) Establish business and funding model chargeback mechanism
	i) Establish Cloud Utilities
	j) Implement change management and capability building programmes
Phase-III Monitoring, management and ongoing improvement	a) Design, implement, monitoring mechanism and review of the overall GI Cloud program
	b) Incorporate suitable modifications as per learning or change requirements

11. Annexure I: Key takeaways from international government cloud initiatives

Most governments are looking to explore cloud computing as a new model of delivering services and improving efficiency of its ICT operations. The government's adoption of cloud is happening at a slower rate than the private sector. However, it is expected to accelerate. Internationally, governments are exploring the option of public cloud for non-critical applications, as follows:

	Private Cloud	Public Cloud
Federal Government Cloud Initiative	Yes	Yes
UK Government Cloud Initiative	G-Cloud	Yes
EU Cloud Initiative	Yet to come out with a strategy	
Australia Cloud Initiative	Yes	Yes
Singapore Cloud Initiative	Central G-Cloud and agency cloud	Yes

Internationally, governments are looking at a 'Cloud Federation' comprising private cloud (or the central government cloud for critical applications), public cloud (for non-critical applications) and sometimes agency cloud. The key focus areas have been–data loss, data protection, security and privacy, data jurisdiction, standardisation, governance, copyright, legal and commercial issues. Governments are involved in various enabling, research and development activities such as NIST, ENISA, etc.

12. Annexure II: Gartner Hype Cycle for Cloud Computing 2012

It identifies various aspects of cloud computing and which state of adoption they are in at present and expected timeframe for main stream adoption.

E.g., while 'cloud advertising' is closer to the plateau of productivity than 'virtualisation', the former has two to five years for mainstream adoption while the latter has less than two years. This essentially means that the market penetration of 'virtualisation' is higher, while even though the maturity of technology and business model of 'cloud advertising' is higher, its market penetration is lower.

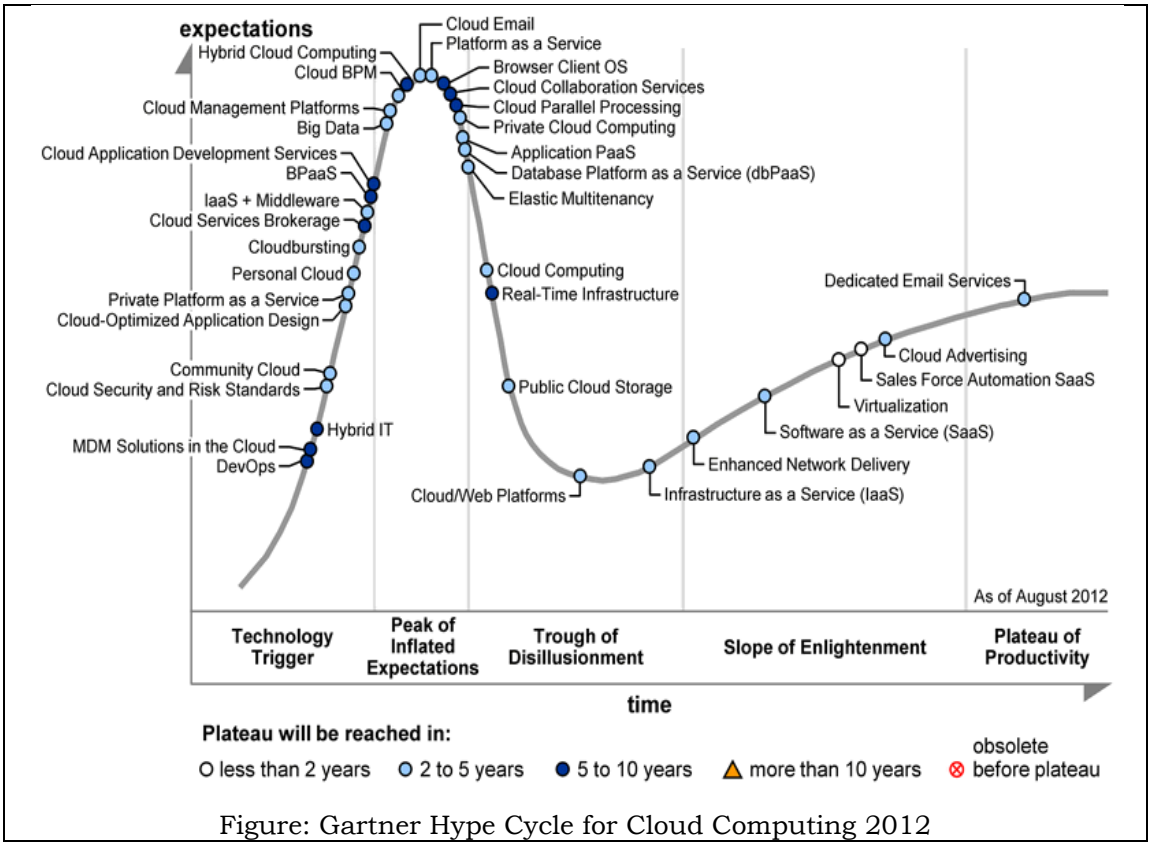

Figure: Gartner Hype Cycle for Cloud Computing 2012

'Cloud computing' is in the trough of disillusionment while 'private cloud computing' is in the peak of inflated expectation. Both are two to five years away from main stream adoption. This signifies the fact that cloud computing is yet to mature both in terms of technology or business readiness and adoption by market.

13. Annexure III: NIST Definition of Cloud Computing

Essential characteristics of cloud computing

The Government of India has adopted the following five essential characteristics of cloud computing as defined by NIST, and generally accepted by industry.

1. **On-demand self-service**: A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
2. **Broad network access**: Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
3. **Resource pooling**: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or data centre). Examples of resources include storage, processing, memory, and network bandwidth.
4. **Rapid elasticity**: Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.
5. **Measured service:** Cloud systems automatically control and optimise resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and

reported, providing transparency for both the provider and consumer of the utilised service.

Cloud computing service models

The Government of India has adopted the three basic types of cloud service offerings as defined by NIST, and generally accepted by industry.

Cloud service models	Description
SaaS	The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings.
PaaS	The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
IaaS	The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Cloud computing deployment models

There are four basic cloud deployment models, as outlined by NIST, which relate to who provides the cloud services. The Government of India may employ one model or a combination of different models in delivery of applications and business services.

Cloud deployment models	Description
Private cloud	The cloud infrastructure is provisioned for exclusive use by a single organisation comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organisation, a third party, or some combination of them, and it may exist on or off premises.
Community cloud	The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organisations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organisations in the community, a third party, or some combination of them, and it may exist on or off premises.
Public cloud	The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organisation, or some combination of them. It exists on the premises of the cloud provider.
Hybrid cloud	The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardised or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

14. Annexure IV: GI Cloud Task Force Constitution

Constitution of the GI Cloud Task Force includes the following:

- Additional Secretary (e-Gov), DeitY, Chairman
- National Informatics Centre (NIC)
- Department of IT, Govt. of Maharashtra
- Centre for e-Governance, Government of Karnataka
- National Institute for Smart Government (NISG)
- C-DAC, Mumbai
- C-DAC, Chennai
- National e-Governance Division (NeGD)
- Bharat Sanchar Nigam Limited (BSNL)
- Ministry of Law
- NASSCOM
- IIIT Bangalore
- Gartner
- CISCO
- Microsoft
- HP
- TCS

15. Glossary

Term	Definition
Agility	In business, agility means the capability of rapidly and cost efficiently adapting to changes. See agile enterprise.
Cloud	A metaphor for a global network, first used in reference to the telephone network and now commonly used to represent the Internet.
Cloud computing	It refers to style of computing in which various resources—servers, applications, data, and other often virtualised resources—are integrated and provided as a service over the Internet. Cloud computing isn't a new technology nor a new architecture. It is a new delivery model.
Cloud computing services	Cloud providers fall into three categories: software-as-a-service providers that offer web-based applications; infrastructure-as-a-service vendors that offer Web-based access to storage and computing power; and platform-as-a-service vendors that give developers the tools to build and host Web applications.
Cloud portability	The ability to move applications and data from one cloud provider to another. See also vendor lock-in.
Cloud provider	A company that provides cloud-based platform, infrastructure, application, or storage services to other organisations and/or individuals, usually for a fee.
Cloud services	A delivery model for information services for businesses and individuals that build on a cloud platform to create dynamic processes and applications.
Cloud storage	A service that allows customers to save data by transferring it over the internet or another network to an offsite storage system maintained by a third party
Pay-per-use pricing model	A pricing model whereby the service provider charges its customers based on the amount of the service the customer consumes, rather than a time-based fee. For example, a cloud storage provider might charge per gigabyte of information stored. See also subscription-based pricing model.
Customer self-service	A feature that allows customers to provision, manage, and terminate services themselves, without involving the service provider, via a Web interface or programmatic calls to service APIs.
Elastic computing	The ability to dynamically provision and de-provision processing, memory, and storage resources to meet demands of peak usage without worrying about capacity planning and engineering for peak usage.
External cloud	Public or private cloud services that are provided by a third party outside the organisation.
Federation	Act of combining data or identities across multiple systems. Federation can be done by a cloud provider or by a cloud broker.
Governance	Governance refers to the controls and processes that make sure policies are enforced.
Grid computing	It is applying the resources of many computers in a network to a single problem at the same time - usually to a scientific or technical problem that requires a great number of computer processing cycles or access to large amounts of data.
Hosted application	An internet-based or web-based application software program that runs on a remote server and can be accessed via an Internet-connected PC or thin client. See also SaaS.

Integration	Integration is the process of combining components or systems into an overall system. Integration among cloud-based components and systems can be complicated by issues such as multi-tenancy, federation and government regulations.
Intercloud	The intercloud is a 'cloud of clouds'. Both public and private versions (intraclouds) not only co-exist, but interrelate. Intraclouds (private clouds) will exist for the same reasons that intranets do: for security and predictability.
Internal cloud	A type of private cloud whose services are provided by an IT department to those in its own organisation.
Interoperability	Interoperability is concerned with the ability of systems to communicate. It requires that the communicated information is understood by the receiving system. Interoperability is not concerned with whether the communicating systems do anything sensible as a whole. (The definitions of interoperability, integration and portability are based on the work at http://www.testingstandards.co.uk/interop_et_al.htm.) (NIST)
Location-independent resource pooling	Resource pooling allows a cloud provider to serve its consumers via a multi-tenant model. Physical and virtual resources are assigned and reassigned (NIST)
Measured service	In a measured service, aspects of the cloud service are controlled and monitored by the cloud provider. This is crucial for billing, access control, resource optimisation, capacity planning and other tasks.
Middleware	Software that sits between applications and operating systems, consisting of a set of services that enable interoperability in support of distributed architectures by passing data between applications. So, for example, the data in one database can be accessed through another database.
Multi-tenancy	Property of multiple systems, applications or data from different enterprises hosted on the same physical hardware. Multi-tenancy is common to most cloud-based systems.
On-demand service	A model by which a customer can purchase cloud services as needed; for instance, if customers need to utilise additional servers for the duration of a project, they can do so and then drop back to the previous level after the project is completed.
Pay-as-you-go	A cost model for cloud services that encompasses both subscription-based and consumption-based models, in contrast to traditional IT cost model that requires up-front capital expenditures for hardware and software.
Policy	A policy is a general term for an operating procedure. For example, a security policy might specify that all requests to a particular cloud service must be encrypted.
Rapid elasticity	Elasticity is defined as the ability to scale resources both up and down as needed. To the consumer, the cloud appears to be infinite, and the consumer can purchase as much or as little computing power as they need.

Reuse	Reuse of pre-existing software has been the Holy Grail of software engineering for years (e.g., subroutines, code libraries, patterns, object inheritance, components and frameworks). In the world of service-oriented architecture, reuse goals take a major step forward through designing services that are abstract, stateless, and autonomous loosely coupled. And the key is that the abstractions of services represent reusable business process segments, not just reusable software. Those process segments can be reused as companies design innovative business processes as "situational" business processes "situational business processes" across for multiple business channels. That is, they can be adapted to completely new business situations. So it is that software flexibility and reuse enables business process flexibility and reuse "reuse." That's the stuff of business agility in hyper-competitive markets.
Service migration	The act of moving from one cloud service or vendor to another.
Service provider	The company or organisation that provides a public or private cloud service.
Service level agreement (SLA)	A contractual agreement between a service provider and a consumer where the consumer's requirements are specified and a service provider defines the level of service, responsibilities, priorities, private and security and guarantees regarding availability, performance, and other aspects of the service.
Ubiquitous network access	It means that the cloud provider's capabilities are available over the network and can be accessed through standard mechanisms by both thick and thin clients. This does not necessarily mean Internet access. By definition, a private cloud is accessible only behind a firewall. Regardless of the type of network, access to the cloud is typically not limited to a particular type of client). (NIST)
Utility computing	Online computing or storage sold as a metered commercial service in a way similar to a public utility.
Web 2.0	The term 'Web 2.0' describes the changing trends in the usage of World Wide Web technology and Web design that aim to enhance creativity, communications, secure information sharing, collaboration and functionality of the Web.
Web 3.0	A supposed third generation of internet-based services. Web 1.0 was read-only, Web 2.0 is read-write, and Web 3.0 'Web 3.0' will be read-write-execute. Web 3.0 (the intelligent Web "the intelligent Web") will involve yet another step-change in how we use the internet and tame the "infoglut". For example, "ontologies" will provide the semantics behind the "Semantic Web" opening up new possibilities for "intelligent agents" to do our bidding, and open "information extraction (IE)" will power new forms of search in a way that avoids the tedious and error-prone tasks of sifting through documents returned by a search engine.
Vendor lock-in	It refers to dependency on the particular cloud vendor and difficulty moving from one cloud vendor to another due to lack of standardised protocols, APIs, data structures (schema), and service models.
Virtual machine (VM)	A file (typically called an image) that, when executed, looks to the user like an actual machine. Infrastructure as a Service is often provided as a VM image that can be started or stopped as needed. Changes made to the VM while it is running can be stored to disk to make them persistent. (NIST)
Virtualisation	The simulation of the software and/or hardware upon which other software runs

Virtual private cloud (VPC)	A private cloud that exists within a shared or public cloud, e.g., the Amazon VPC that allows Amazon EC2 to connect to legacy infrastructure on an IPsec VPN.

16. References

1. DeitY Annual Report 2011-12 available at http://deity.gov.in/
2. NIC Annual Report 2010-11 available at http://www.nic.in/
3. NIST Definition of Cloud Computing, Special Publication 800-145 (Draft)
4. US Government Cloud Computing Technology Roadmap Volume I Release 1.0 (Draft), Special Publication 500-293, available at
5. Cloud Computing Strategic Direction Paper – Opportunities and applicability for use by the Australian Government, April 2011, Version 1.0, Department of Finance and Deregulation, Australian Government
6. IT Reform: "Federal Cloud Computing Strategy" Published, http://www.cio.gov/
7. UK Government ICT Strategy resources, http://www.cabinetoffice.gov.uk
8. A cloud computing strategy for Europe, JUNE 3, 2012, http://www.neurope.eu/
9. Government Policies on Cloud, DeitY Working Group on Cloud Computing submitted by Data Security Council of India
10. Cloud Computing Strategic Direction Paper, April 2011, Version 1.0, Australian Government, Department of Finance and Deregulation
11. Possible Approach to Creating a National Cloud Computing Platform: Brief for Discussion, Cisco Internet Business Solutions Group (IBSG)
12. Shared Services/Cloud Framework for Accelerating Nationwide Rollout of NeGP MMPs - Approach Paper, Cisco Internet Business Solutions Group (IBSG)