GI Cloud (Meghraj) Adoption and Implementation Roadmap

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 Executive Summary

The Government of India initiated the National e-Governance Plan (NeGP) in May 2006 with a vision to make all government services accessible to citizens in their own locality, through common service delivery outlets at affordable costs. While ICT infrastructure is being put in place by states with funding and assistance from the central government, the deployment of application software, even after outsourcing it completely, has been tardy. The problem has been the elaborate procurement process to be followed and lack of expertise within departments to handle such large-scale procurement and application development initiatives. The government wants to accelerate implementation through the development and use of a shared applications platform.

The aim is to realise a comprehensive vision of a government private cloud environment available for use by central and state government line departments, districts and municipalities to accelerate their ICT-enabled service improvements (the NeGP Mission Mode Projects and other applications), to support the cost-effective ongoing maintenance and evolution of the underlying ICT-enabled environment, and to support the overall vision of the NeGP, (i.e. improved government services to the common man).

In pursuit of the vision, the Department of Electronics and IT (DeitY) has embarked upon a National Cloud initiative termed as 'GI Cloud'. A task force has been set up to give necessary direction with respect to the various activities which include creation of a detailed plan on the cloud strategy, cloud architecture, cloud implementation plan and roadmap.

This document provides a roadmap for tapping the massive benefits on offer through enabling a cloud based computing environment across the country. It is to be read along with the 'GI Cloud – Strategic Direction paper', which addresses the strategy aspects of this initiative.

This roadmap document covers the brief study done to understand the present government ICT initiatives and provides an assessment of the current government ICT infrastructure. The objective is to understand the government's existing position in terms of IT enablement.

The present assessment has helped to define the GI cloud architecture in the subsequent sections.

Section 3 defines an architectural vision and the GI Cloud environment. This section identifies the components of the GI Cloud viz. National and State Clouds, the eGov AppStore and the services that will be available from them.

Section 4 describes the eco-system of the GI Cloud environment and the role of each stakeholder in the eco-system and the identification of bodies fulfilling the mentioned roles.

Section 5 captures the institutional set up of GI Cloud. It details out the functions of the bodies under the institutional set up required for successful operations of the GI Cloud.

Section 6 elaborates the capacity and capability building requirements for GI Cloud. It defines a plan for gap assessment between present capability and the required capability and provides a change management and augmentation plan.

Section 7 is focussed on the business model of GI Cloud and it discusses the need for revised government procurement norms for cloud computing.

Section 8 describes the implementation plan. It defines the implementation principles and identifies the list of strategic initiatives required for GI Cloud. It prioritises the identified initiatives and defines the sequence in which these initiatives need to be implemented. Finally it discusses the envisaged challenges for implementation.

2 Assessment of Current Government ICT Infrastructure and National Information Infrastructure

The National e-Governance Plan (NeGP) takes a holistic view of e-Governance initiatives across the country, integrating them into a collective vision, a shared cause. Around this idea, a massive countrywide infrastructure reaching down to the remotest of villages is evolving, and large-scale digitisation of records is taking place to enable easy, reliable access over the internet. The key pillars of the infrastructure under NeGP include – State Wide Area Networks (SWAN), State Data Centres (SDCs), National Service Delivery Gateway (NSDG), State Service Delivery Gateways (SSDGs) and Common Service Centres (CSCs).

Along with the infrastructure that is being built as part of the NeGP, other initiatives like National Data Centres (NDCs) by NIC, National Knowledge Network (NKN) and National Optical Fibre Network (NOFN) are also in progress.

A snapshot of these ICT infrastructure initiatives by the government has been provided below to understand their current implementation status:

Under Central Government:

- Large NDCs are run by NIC at Delhi, Hyderabad and Pune. Another NDC is being set up at Bhubaneswar.
- The NDC at Shastri Park, Delhi is at an advanced stage of virtualisation and is the largest government data centre.

Under State Government:

- SDCs in 21 states have been made operational and SDCs in four states are in an advanced stage of implementation.
- Currently, in about ten of these SDCs, the utilisation of infrastructure has reached more than 50%. The 21 SDCs are running a number of applications such as commercial tax, e-Procurement, Bhoomi, mandi board etc. Line departments of these states are happy to get reliable and secure services from the State Data Centre.

- Effort is in progress to enable SDCs to adopt virtualisation and cloud computing. The SDC at Maharashtra is at an advanced stage of cloud adoption.

Networks (both Central and State Government):

- Existing network infrastructure includes SWAN, NKN, NICNET and NOFN.
- Implementation of SWAN is in full swing and SWANs in 30 states have been operational.
- For around 10 to 15 states, SWAN has been integrated with NKN.
- NOFN is expected to be completed by 2014-15. The scope of NOFN is to address the connectivity between gram panchayats and blocks by laying incremental cable from the block level to the gram panchayat level.
- As stated above, the core ICT infrastructure of the government has now been largely implemented and is operational. So it is being considered appropriate to plan for a National Information Infrastructure 2.0 (NII 2.0). NII 2.0 would be significantly upgraded on technological, administrative and e-Governance perspectives, while seeking to optimise the utilisation of the available core infrastructure with the central and state governments. The focus of the proposed NII 2.0 initiative is on integration of networks, data centres, cloud computing and network security. Within the overall integrated institutional structure of NII 2.0, there would be a specialised mechanism or entity to address the specific issues related to implementation of GI Cloud.

3 GI Cloud Architecture

To adopt cloud computing by the government, it is imperative to identify an architecture which will provide the benefits as envisaged from the cloud computing environment.

This architecture needs to take into consideration the investments that have already been made by the government on building infrastructure both at the national as well as state levels. These include data centres at the national and state levels, the network backbones available through SWAN, NKN, NICNET and the middleware gateways e.g. NSDG, SSDG.

3.1 Architecture Vision

The architectural vision of GI Cloud centres 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 GI Cloud Services Directory. The key element is the development of government cloud architecture to provide the high-level blueprint of ICT enabling various government functions at national, state, district and municipal levels. In this vision, the government cloud architecture would comprise of multiple private cloud computing environments at the national and state levels.

In line with this vision, establishing the envisaged cloud computing environment requires neither a single implementation service provider nor a single technology vendor. Instead, so long as the right steps are taken to align government ICT procurement practices with the cloud computing vision and architecture, healthy competition can exist with availability of a standardised platform facilitating the development and maintenance of cloud-based applications faster and more cost effective. If the software and tools contained in this cloud environment are based on open standards, the risk of technology and vendor lock-in is mitigated since multiple vendors can compete for a given element of the platform.

It would also contain a layer of support services enabling multiple stakeholders to participate in a coordinated fashion and share costs as desired. The support layer includes a help desk to provide timely and consistent help to all stakeholders and to

serve as a focal point for capturing and disseminating cloud best practices and ensure adherence to government defined guidelines and standards for GI Cloud. A dashboard would provide real-time visibility into operational status and metrics across all participants in the cloud, enabling quick issue resolution and informing effective decision-making about future evolution.

3.2 GI Cloud Environment

The GI Cloud environment is envisaged to be initially established – building on the infrastructure investments already made or augmentation of the same – by the creation of discrete cloud computing environments at the national and state levels termed as 'National Clouds' and 'State Clouds' respectively. While one of the National Cloud will be built utilising the infrastructure available under the NDCs, the other clouds at the national level may be established with new or augmentation of existing data centres available at the state level. This will be done keeping in view the scale of requirements identified after demand assessment, application sensitivity and data classification study. In line with the architectural vision, the figure here provides an overview of the GI Cloud wherein in addition to the establishment of multiple National Clouds, willing State Clouds built on state data centres can also become part of the GI Cloud environment and publish their cloud services in the GI Cloud Services Directory. There may be states and union territories with their own SDCs and State Clouds existing outside the GI Cloud. Over a period of time, the IT infrastructure across the country is expected to be consolidated and interconnected.

Based on the demand assessment and taking into account security related considerations, government may also engage the services of private cloud providers.

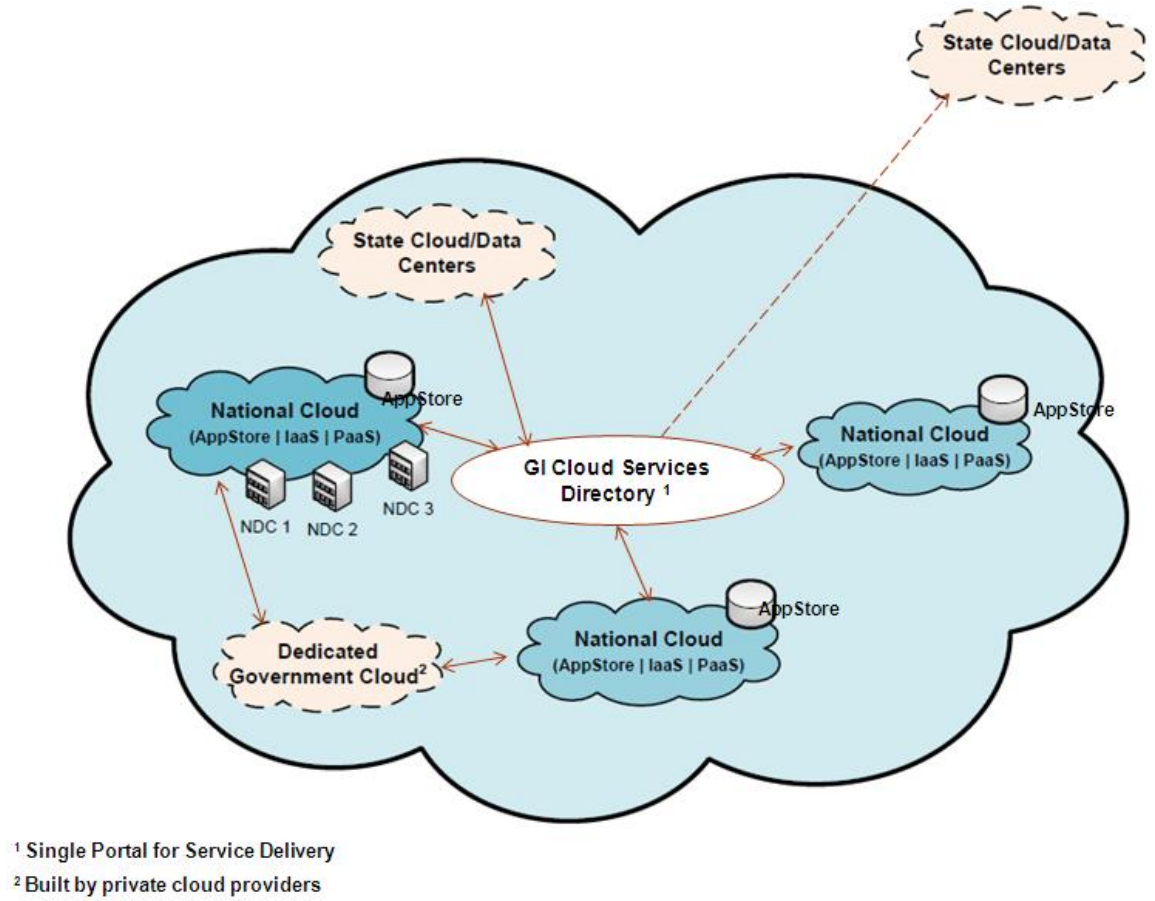


Figure 1: GI Cloud Environment

Initially, one National Cloud will be set up and after assessing the demand, application sensitivity and data classification, other clouds at the national level may be set up later. Services provided by National Clouds could include infrastructure (compute, storage and network), platform, backup and recovery, infrastructure scaling of the State Clouds, application development, migration, hosting etc. As stated earlier, the state data centres can also associate with GI Cloud either by acting as independent cloud environments or by lending their IT Infrastructure as part of GI Cloud. However, in both the scenarios, the state data centres will have to adhere to the standards and policy guidelines of GI Cloud and publish their cloud services through the GI Cloud Services Directory. Over a period of time, states may decide to hand over the entire infrastructure management and operations of its SDC cloud infrastructure or other state ICT infrastructure like SWAN to any of the agencies or entities managing the National Clouds. These entities at the national level could also act as remote infrastructure management of the State Clouds.

As stated earlier, inclusion into the GI Cloud is not a mandate. There can be states and union territories having their own SDCs and State Clouds existing outside the

GI Cloud eco-system. States and union territories will be encouraged to leverage the GI Cloud resources as and when they have exhausted their own resources available under their data centre. This will bring the benefit of optimum utilisation of resources both at the SDCs as well as at the cloud environments being set up under GI Cloud.

National Cloud services

The National Clouds will be equipped to provide cloud services, i.e. IaaS, PaaS and SaaS. An indicative list of cloud-based services has been provided below:

- Infrastructure-as-a-service (IaaS):
    - Compute as a service
    - Storage as a service
    - Network as a service
    - Disaster recovery as a service
    - Backup as a service
    - Virtual desktop solutions
    - High availability services
    - Infrastructure for application development and testing
    -
- Platform-as-a-service (PaaS):
    - Platform for application, portal development and testing
    - Platform for application or portal hosting
    - Database as a service
    - Collaboration platforms
- Software-as-a-service (SaaS): Applications (core applications and common applications like payment gateway, messaging platform, MIS reporting etc) can be made available by GI Cloud through the respective eGov AppStores or in a pure SaaS model. The eGov AppStores will host both cloud and non-cloud enabled applications. Consumers will have the option to download an application from the eGov AppStores or run it directly from the cloud. Indicative SaaS services include the following:
    - Email as a service
    - Productivity suites (as a service)
    - ERP as a service
    - CRM as a service

- BI and analytics as a service
- Collaboration as a service
- Identity and assess management (IAM) as a service
- Security as a service
- Common central services like payment gateway, mobile gateway, PKI, etc as a service

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

The entire set of services shall be published through a single window or portal – the GI Cloud Services Directory. This will provide a single window for discovery of services and related information to the consumer.

It is also pertinent to clarify that the cloud services envisaged for GI Cloud are different from the end-user services like services delivered through various MMPs like e-District, Passport, eSeva Project, MCA21 and Income Tax, and other national or state projects like UIDAI.

3.2.1. eGov AppStore

National eGov AppStore

The eGov AppStore will include the setting up of a common platform to host and run applications (developed by government agencies or private players) at National Clouds, which are easily customisable and configurable for reuse by various government agencies or departments at the central and state levels without investing effort in the development of such applications. The eGov AppStore hosted on the National Clouds will be termed as the 'National eGov AppStore'.

eGov AppStore Eco-System

The eco-system of the eGov AppStore consists of the following actors:

- Application Owner: These are entities responsible for providing applications to be hosted on an eGov AppStore. These could include any government department at central and state level or private players providing reusable applications that are cloud-ready or can be made cloud-ready. They may also be responsible for productisation of the non-cloud ready applications.
- Application Provider: It is the entity (government department or independent entities) that will be responsible for hosting and providing services through the respective eGov AppStore. The agencies or entities responsible for operations of the National Clouds could also act as the application provider for the respective National eGov AppStore.

  Responsibilities of the application providers for the eGov AppStores include the following:
  - Identification and selection of applications for hosting on the respective eGov AppStore based on DeitY guidelines
  - Hosting of these applications on the respective cloud environment and maintenance of the same
  - Managing contractual agreements with the application consumer and application owner
  - Evolving business model for service delivery to the consumers
  - Setting up of AppStore Management Unit
  - Negotiating and making the price of each service and performance rating visible in the GI Cloud Services Directory for comparison, promoting competition and service excellence
- Empanelled Agencies: DeitY will empanel agencies for specific functions, which include the following:
  - Certification and accreditation of applications for hosting on the eGov AppStores
  - Application development and customisation
  - Imparting training and conducting capability and awareness creation programmes
- Application Consumer: The consumers of the eGov AppStores include government departments, citizens or private sector organisations using the application from the respective eGov AppStores either by downloading the application or running in a SaaS model. Application consumers can be categorised into the following two groups:

- Direct Users: These consist of users who are access the applications directly from the eGov AppStores, e.g. departments, government officials at the central and state levels running email applications at the eGov AppStores, state department running e-district application through the eGov AppStore.
- Indirect Users: These consist of the end users of services provided through these applications, e.g. government officials using email services provided through the eGov AppStores, citizens accessing services provided through e-district application.

Hosting of eGov AppStore

As stated earlier, more than one application store can exist in the GI Cloud ecosystem. However, there will be a single window or portal or service catalogue – the GI Cloud Services Directory – displaying the various applications and services of each of the eGov AppStores. It will also provide technical information such as the technology stack used in the application, the user manual and other relevant documents. It will also provide non-technical information such as types of services delivered, implementing agency and owner agency related to each application.

eGov AppStore Services

Core and common applications that have high demand and are replicable across the central and state levels are the likely candidates for eGov AppStores. Common components like the payment gateway, messaging platform, MIS reporting, etc, will also be made available in the GI Cloud through the eGov AppStores.

The eGov AppStores will host both cloud enabled and non-cloud applications. This will make available of applications that have not yet matured to a cloud environment, but can be readily deployed and utilised by other departments at the central and state levels with suitable customisations. Periodically, an assessment will also be conducted for feasibility of enabling non-cloud applications to cloud-based architecture.

Any department can use the services of eGov AppStores through two primary means – either by directly running the application available in the respective eGov AppStore or by downloading the application from the respective eGov AppStore. For complex applications that require major modifications to be used by different states, only a

productised version whose core is downloadable will be available at the eGov AppStores. However, for generic applications that can be used by multiple departments at the central and state level, limited modification options will be provided for running them from the cloud or downloading and running from the respective eGov AppStore.

4 Eco-system

The eco-system of the GI Cloud identifies the major actors, their activities and roles in the envisaged cloud computing environment. The Conceptual Reference Model of NIST has been referenced for depicting the high-level eco-system of GI Cloud, as shown below.

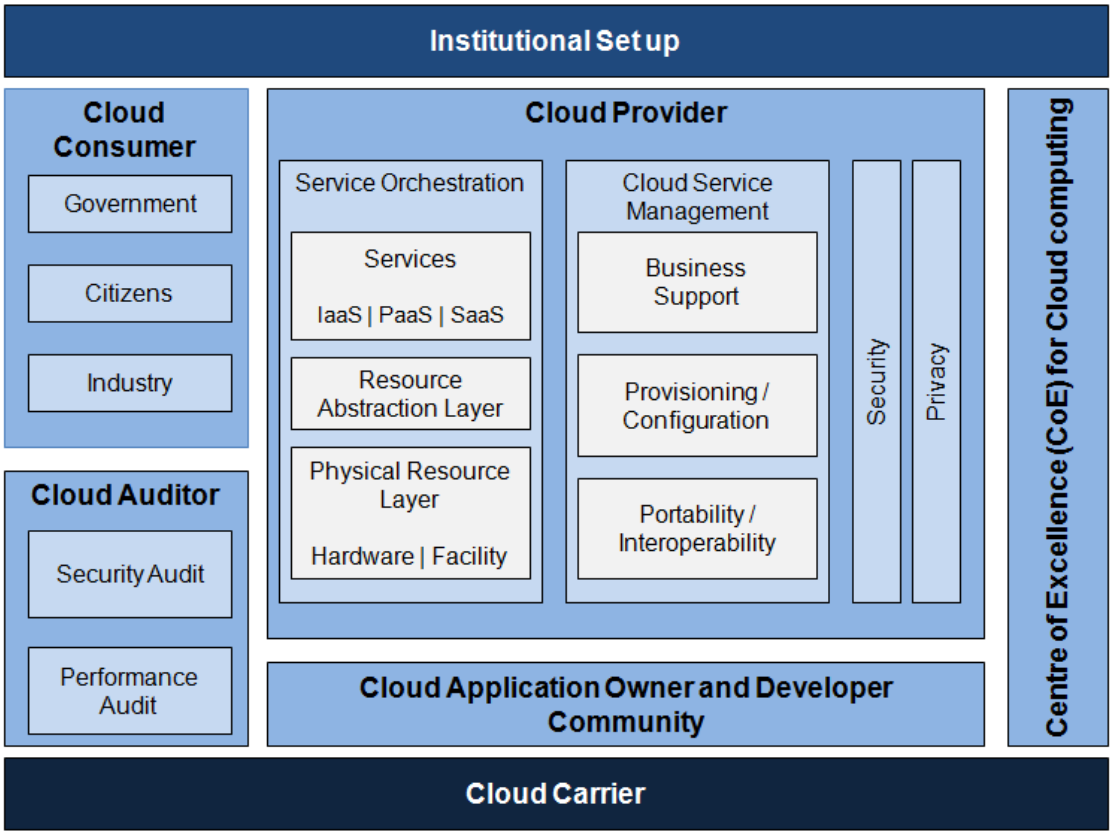


Figure 2: GI Cloud Eco-System

Eco-system actors

The GI Cloud eco-system defines eight key actors in the envisaged GI Cloud Environment (as defined under the section 'GI Cloud Architecture'). These actors include: the Institutional Set up, Cloud Consumer, Cloud Provider, Cloud Auditor, Cloud Carrier, Centre of Excellence (CoE) for Cloud Computing and Cloud Application Owner and Developer Community. Each of these actors is an entity (a person or an organisation) or a community that participates in the eco-system, and has specific roles and performs specific tasks.

4.1 Institutional Set up

The Institutional Set up consists of the following entities:

- An Empowered Committee under the chairmanship of the Secretary, DeitY with representation Central/State ministries and other government entities;
- Architecture Management Office (AMO).

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.

Details of each entity defined in the Institutional Set up and their responsibilities have been covered under the section 'Institutional Set up'.

4.2 Cloud Consumer

The Cloud Consumer is the principal stakeholder that uses or consumes the GI Cloud services. The Cloud Consumer browses the GI Cloud Services Directory, requests the appropriate service, sets up service contract with the respective cloud provider and uses or consumes the service. Based on the services consumed from the GI Cloud, the cloud consumer may need to arrange for payments. Consumers of the envisaged GI Cloud include citizens, government departments, line departments and agencies at the central and state levels.

4.3 Cloud Provider

The Cloud Provider is an entity that is responsible for operating the respective cloud environment and makes available GI Cloud services to interested parties.

Responsibilities of the cloud provider include the following:

- Acquiring and maintaining infrastructure required for providing services
- Implementing measures for adherence to cloud standards
- Operating the respective cloud computing environment
- Protecting the security and privacy at required levels
- Providing cloud computing services and service elastic workloads based on the requirement of cloud consumers
- Adhering to service level agreement (SLA)
- Issuing bills and collect payments

- Executing contract management
- Forecasting demand for cloud services
- Following the government of India laid policy guidelines and standards

It is envisaged that one of the National Clouds will be established and managed by a national government agency and the other clouds at the national level will be established and managed by separate Cloud Utilities. These Cloud Utilities will be a class of institutions set up to handle all aspects of operations and service delivery of the other clouds at the national level. These institutions would work in the spirit of partnership with government, which help them overcome operational challenges, providing necessary agility and flexibility required in managing the dynamic environment of GI Cloud.

4.3.1. Cloud Utilities

Role of Cloud Utilities

The Cloud Utilities will act as the service providers of the GI Cloud through the respective cloud computing environments at the national level. Initial seed funding may be provided by DeitY depending upon the choice of Cloud Utility for setting up of the respective cloud environments at the national level. However, it is envisaged that Cloud Utilities will be independent entities and will sustain themselves by earning profits.

Major role of the Cloud Utilities for other clouds at national level includes the following:

- Acquiring or using existing infrastructure for set up (including the respective eGov AppStores)
- Running, operating and managing entire operations
- Provisioning of services (IaaS, PaaS and SaaS)
- Identification and selection of application for hosting on the respective eGov AppStores
- Developing new applications and provide them as service
-
- Providing support services for application development and productisation
- Training of staff and handholding after cloud migration

Number of Cloud Utilities

It is recommended that separate Cloud Utilities are established for set up, operations and maintenance of each of the cloud computing environments at the national level. Each of these Cloud Utilities will act as independent cloud providers of the GI Cloud. Some key advantages of establishing multiple Cloud Utilities are as following:

- Ensuring healthy competition
- Curtailing monopolistic tendencies
- Ensuring better service delivery
- Accelerating progress

These entities will have pan-India footprint and will operate in any state or union territory, thus competing with each other.

Should new Cloud Utilities be established?

The existing State Nodal Agencies (SDAs), national government agency, private organisation or National Information Utilities (NIU) like NSDL, NPCI, etc can be leveraged to operate the cloud computing environments at the national level instead of establishing new Cloud Utilities. However, the feasibility of the same needs to be assessed by understanding the following:

- What specialised competency would be required for running and operating the envisaged cloud environments at the national level?
- Do the existing entities have the required competency? Do they have the required man power and skills?
- Can the existing entities develop or acquire the desired competency and skills? How long will it take for them to do so?
- Do the existing entities have required flexibility to operate including hiring or technical manpower at market rates?

If the feasibility study suggests that a new Cloud Utility should be established, the same can be done by preferably setting up a private company (section 25 company) with a public purpose.

Constitution or Establishment of new Cloud Utility

The new Cloud Utility could be a private company (section 25 company) with a public purpose, which aims at profit making but not profit maximising. The structure of the Cloud Utility should be such that it works without the need for day-

to-day guidance and advisory from the shareholders, members or board. The management should be independent and empowered to take quick and efficient business decisions pertaining to attracting and retaining talent, procurement, rapid response to business exigencies, adopting new technologies, etc. The independence of the management is linked to the financial independence of the Cloud Utility. Therefore, the Cloud Utility should be able to get funding independently and have a self-sustaining financial model. If required a seed funding could be given by DeitY.

The following are desirable features for effective functioning of the Cloud Utility:

- **Self-financing**: The Cloud Utility should be capable of self-financing its operations and providing for its sustenance in the near future.

- **Make reasonable profits**: The Cloud Utility should endeavour to generate reasonable profit in order to be self-sustaining. It should levy reasonable charges on its users without abusing its dominant position and must not maximise profit or valuation. Salaries of employees should not be linked to profits. The salaries should be competitive and market driven, to ensure that the best candidates for the job can be hired.

- **Net worth**: The net worth of the Cloud Utility should be available as a last resort to meet exigencies and ensure that it is able to sustain itself as a going concern.

- **Professional standards and competitive practices**: It must maintain the same professional standards in all its dealings, including its dealings with competitors, technology providers and related entities. It must be able to maintain its integrity by being unbiased while dealing with all such entities.

- **Transparency**: It should maintain utmost transparency in its operations and should at least make disclosures that are mandated for a listed company on its website.

- **Technology**: It should be willing to invest in technology for increasing efficiency, reach and economies of scale.

- **Competition**: Establishing a Cloud Utility would have characteristics similar to those of private entities but with a public purpose. Hence, it is essential to

create enabling conditions that allow multiple Cloud Utilities to exist over a period of time.

4.4 Cloud Auditor

Responsibilities of the Cloud Auditor are as follows:

- Conducting independent audit of security, privacy and performance of GI Cloud
- Risk and compliance assessment to determine alignment to regulatory mandates
- Publishing independent audit report
- Certifying the cloud environments as per Government of India defined norms and guidelines

The audit reports will be presented to DeitY, which will process the same and take remedial actions and steps based on the audit reports.

4.5 Cloud Carrier

The Cloud Carrier acts as an intermediary and provides the network connectivity backbone for transport of cloud services between cloud consumers and cloud providers of GI Cloud.

The infrastructure backbone for the GI Cloud will be provided by existing networks like SWAN, NKN, NOFN and NICNET. It is envisaged that a National Information Infrastructure (NII 2.0) for the country will be established through seamless operations of the core government ICT infrastructure (network, data centre and security) The NII 2.0 would provide a unified and secure network to the cloud entities within the GI Cloud.

4.6 Centre of Excellence for Cloud Computing

Establishment of CoE

Keeping in view the fact that the concept of cloud computing is new and ICT capacity is low in Government agencies it is envisaged that one or two Centres of Excellence (CoE) for Cloud Computing will be established at the national level with

the purpose of realising the cloud computing vision of the Government. The CoE's role will be crucial in terms of capability building, providing advisory and spreading awareness within the Government about cloud and its benefits apart from international collaboration and coordinating research and development in this area. The CoE could also be entrusted with the task of housing the Architecture Management Office (AMO).

Role of the CoE

The role of the CoEs would be to provide the following services:

- Advisory Services: This would include providing advisory services to various departments and agencies at central and state level for migration of the existing applications and development of new applications using the cloud computing technologies. Envisaged activities would include the following:
    - Providing strategic advice in the design and implementation of cloud-based applications to the government departments and states
    - Design cloud roadmap for the government departments and agencies
    - Supporting the central and state governments in designing large cloud computing projects cutting across departments and ministries, developing models and framework for monitoring and evaluation of projects, etc.
- Awareness Creation: This would include creation of awareness of cloud computing across the Government departments and agencies in central and state level. Envisaged activities would include:
    - Showcasing of successful cloud technologies and applications,
    - Conducting workshops, orientation sessions etc.
- Capacity Building: This would include establishing an institutional framework, engaging personnel with required skill sets and experience and upgrading internal skill sets through training. Envisaged activities would include the following:
    - Institutional capacity building
    - Developing institutional partnerships
    - Knowledge management
    - Training and change management programmes, etc.

- Research and innovation: This would include research and development activities into critical areas of cloud computing like inter-operability, data portability, standards, etc. Envisaged activities would include the following:
    - Collaboration and liaison with international research bodies and agencies like NIST, etc
    - Developing expertise in various cloud platforms, establishing SLAs, porting different applications on different platforms making these platforms interoperable with each other
    - Creating the best practices and guidelines.

4.7 Cloud Application Owner and Developer Community

Cloud Application Owners and Developer Community are government or private entities and communities that provide or develop reusable cloud ready applications that can be hosted on the GI Cloud environment for use by the consumers of GI Cloud.

5 Institutional Set up

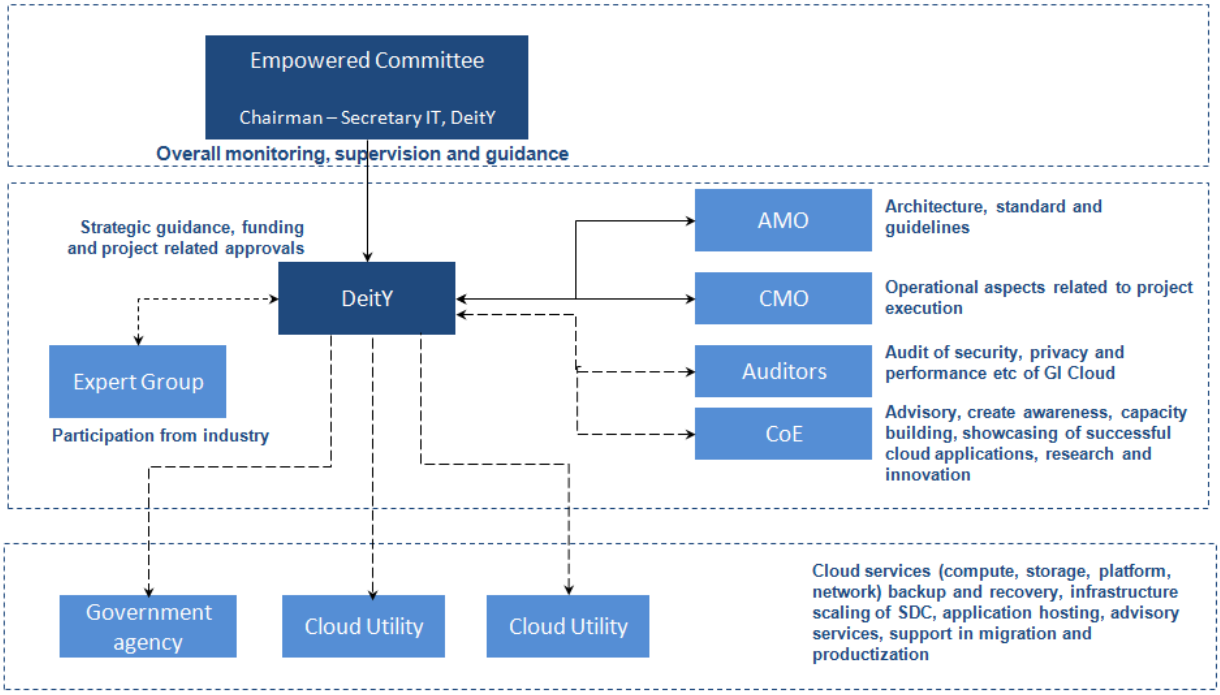


Figure 3: GI Cloud Institutional Set up

The institutional set up for GI Cloud is represented in the figure above. It consists of the following:

- Empowered Committee
- Architecture Management Office (AMO)
- 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.

5.1 Empowered Committee

Establishment of Empowered Committee

The Empowered Committee for GI Cloud is a committee with decision making and approval authority formed under the Chairmanship of Secretary, DeitY, with representation from Central/State ministries and other government entities. The Empowered Committee will be serviced by DeitY.

Role of the Empowered Committee

Major functions of the Empowered Committee will include the following:

- Setting vision
- Providing strategic and regulatory direction and guidance to all the stakeholders
- Laying down common set of guidelines and standards for GI Cloud
- Dispute resolution and timely intervention as and when required

5.2 Department of Electronics and IT (DeitY)

It is envisaged that the DeitY will primarily have three functions – policy and strategic direction, operational management, architecture guidelines and standards creation. Separate specialised units will be established, viz. the Architecture Management Office (AMO) to assist in formulation of architecture guidelines and standards and Cloud Management Office (CMO) responsible for management and monitoring of the entire GI Cloud initiative. DeitY will function under the strategic guidance of the Empowered Committee and will have the following major functions:

- Policy formulation and enforcement
- Steer the GI Cloud initiative
- Demand assessment for the GI Cloud
- Provide seed funding to the agencies for establishment of the National Clouds and the Cloud Utilities
- Monitoring and supervision of the operations of AMO and CMO
- Other approvals related to project execution and funding
- Approval where required for hosting applications on the eGov AppStore
- Capacity building, change management and awareness creation exercise
- Creation of CoE for GI Cloud

Cloud Management Office (CMO)

The CMO will act as a Program Management Office of DeitY and will closely work with AMO, the government agency and the respective Cloud Utilities to ensure smooth implementation and operations of the GI Cloud eco-system. The CMO will report directly to DeitY and will help in co-ordination, management and monitoring of the entire GI Cloud initiative. Major functions of CMO include the following:

- Handling of day-to-day operational aspects related to project execution
- Defining the operational model for all Cloud Utilities

- Assistance in management of disbursal of funds
- Conduct follow-ups, monitoring progress and regular reporting to the Empowered Committee
- Participate in Empowered Committees and other stakeholder forums as needed to ensure alignment with GI Cloud strategy

Architecture Management Office (AMO)

In order to assist DeitY to realise the complete architecture vision of GI Cloud and ensure standardisation across technology, platform and standards the AMO will be established.

The AMO will define and implement architecture guidelines and standards specific to GI Cloud. Major functions of AMO include the following:

- Developing the GI Cloud reference architecture
- Defining guidelines for new application development, architecture, standards, RFP, SLA, contract management, etc in consultation with industry and based on international best practices

5.3 GI Cloud Expert Group

In addition to the Empowered Committee and the various units supporting DeitY, It is proposed to create a 'GI Cloud Expert Group' with experts from the industry to deliberate on the standards/ guidelines prepared by AMO. Major functions of the Expert Group include the following;

- Assistance in development of policies/ guidelines
- Providing inputs in development / implementation of the GI Cloud components
- The expert group will also provide inputs in the various capacity building exercises to be conducted as part of the GI Cloud initiative

6 Capacity Building

For the effective usage of the entire GI Cloud environment, it is important to understand the requisite skills required for monitoring and management of the entire operations of GI Cloud.

The skills thus identified would be required both at the senior management level as well as with the operations team, though there would be a discrete difference in the applicability as per the job functions.

It is with this objective, a summary of the different kind of profiles required has been listed in the Competency Requirements.

6.1 Competency Requirements

The competency requirements of the overall system can be classified into five broad categories required across the spectrum. The below figure depicts the kind of competencies required in a cloud-ready environment, keeping in view the evolvement towards a unified infrastructure environment. However, this doesn't undermine the role of infrastructure and security experts, as required during any data centre operations.

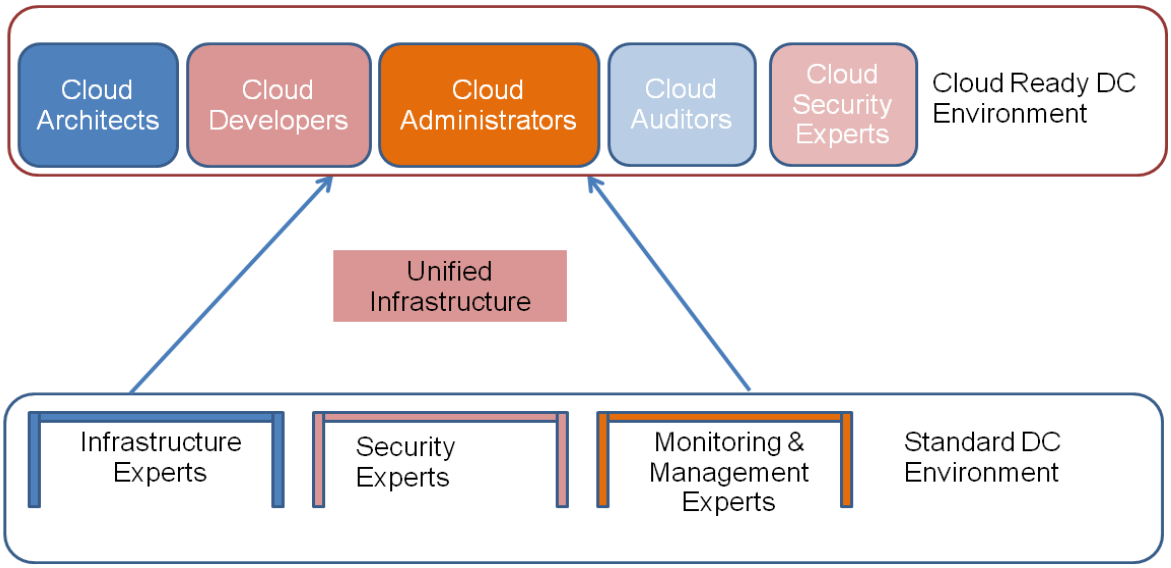


Figure 4: Cloud Ready DC Competency

Cloud Experts	Roles and responsibilities
Cloud Architects	• Designing of cloud architecture for projects • Designing for migration to cloud platform, including assessment of services or applications that needs to be migrated to cloud • Developing cloud implementation roadmap for projects
Cloud Developers	• Any development activity on the cloud platform including application development
Cloud Administrators	• Service provisioning, monitoring and billing and providing reports • Supervision of support and helpdesk operation
Cloud Auditors	• Internal audit of the cloud environment o Performance audit o Financial audit o Security and privacy audit o Compliance audit
Cloud Security Experts	• Cloud security design and implementation • Providing inputs to cloud architects and cloud developers

It is recommended that dedicate teams are created for the above mentioned roles for the identified GI Cloud eco-system stakeholders as depicted below.

Eco-system actors	Expertise in cloud data centre environment
Cloud Provider	Cloud Architects, Cloud Developers and Cloud Administrators
Cloud Consumer	Not applicable
Cloud Carrier	Network experts
Cloud Auditor	Cloud Auditors and Security Experts
Cloud Application Owners	Cloud Architects, Cloud Developers and Cloud Administrators

6.2 Capability Gap Assessment and Augmentation Plan

To understand the required capabilities to be developed a gap assessment of the present environment needs to be done following the methodology depicted below:

Figure 5: Capability Gap Assessment

Present Environment Review

At the central level, the projects managed under DeitY are handled by DeitY along with National e-Governance Division (NeGD) team as well as through the Project Management Units (PMUs). However, the roles of both are limited to the project management level with no possible spare capacity to focus on the new initiatives, as envisaged, to create the GI Cloud environment. Also, the competencies and capability will need to be augmented keeping in consideration the projects that are not under the purview of DeitY but would certainly evaluate and utilise the GI Cloud to run their services. The units suggested under the institutional set up (i.e. AMO and CMO) will certainly play a key role in fulfilling the required capabilities and right skills.

Augmentation Plan

The kind of skill set required for stakeholders need to be scaled up as per the following plan:

- **Centre Level:** A consolidated team of the cloud developers, architects, security experts, auditors and administrators need to be developed at the central level. This will require creation of a pool of resources being sourced either through the industry and identifying the different levels of certification highlighting the competencies of the team.

- **Centre of Excellence (CoE):** As depicted in the report earlier one or two CoE will be established at the national level. The capacity of expertise to be available within CoE shall be defined based on a detailed study of the present assessment of services to be provisioned through GI Cloud.

- **State Level:** As an extension to the initiative to be taken up by the centre for creation of pool of resources, the same capacity building pattern may also need to be utilised for creating the essential expertise at the state level. This also will require taking into account the present competencies available as part of the composite teams at the state level.

6.3 Change Management and Orientation Program

As the Government of India establishes a GI Cloud for enhancement of e-Governance services and speedy implementation of the projects, important functional changes are imminent.

The transition from the current status to the future cloud environment usage will require a mindset change both at the organisational level as well as at the personal level. Hence orientation and change management workshops are essential to catalyse this initiative.

The workshops shall cover the benefits envisaged from utilisation of cloud, issues and challenges, role of major stakeholders, cloud-ready application development, migration of applications to cloud, etc.

The key objectives of such programme shall be the following:

- Making the participants aware of their roles and responsibilities in providing and accessing cloud services
- Tackling some of the challenges of cloud implementation and solutions
- Helping the participants understand the process of change, how they can be a positive force in driving that change, and the best practices for implementing change in an organisation
- Obtaining commitments from top management for enablement of cloud environment
- Addressing the fears and resistance due to new roles and resultant new environment
- Developing affirmative communication and conceptualise motivational strategies

6.4 The Plan

Participants

The primary purpose is to undertake orientation and change management under the capacity building programme for the following officials:

- Centre and State IT Department (acting as providers or users of GI Cloud)
- Nodal agencies

The table below provides an indicative summary of our training approach aimed at conducting the training:

Platforms	**Target Audience**	**Total Officers Identified**	**Min. No. of Days**	**No. of Batches**
Cloud Environment - Orientation and Change Management	Centre and State Departments – • DoIT, • Nodal Agencies, • Cloud Providers, • Cloud Users (departments at centre and state)	To be identified as part of the actual implementation exercise	1 day Workshop	As per the no. of officials with a maximum strength of 15 people per batch
Modules or Technical Training	Nominations by departments at centre and state levels, Other Agencies		6 day Workshop	

7 Business Model

7.1 Business Model

The GI Cloud will 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 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.

With increase in demand for cloud-based services, the government may take a view to invite the private cloud providers to set up dedicated government clouds or empanel private cloud providers based on the policy, standards and guidelines for GI Cloud.

a. National Cloud

At the Central Government level, National data centres will be set up to host the central and state government applications. Different business models can be provided, such as pay-per-user, subscription, or offering services free of cost as per the guidelines of DeitY. The National Cloud will be owned and run by a Central Government agency.

b. Other clouds at the National level

As elaborated in the institutional set up section, the other clouds set up at the national level will need to be managed and operated by their respective Cloud Utilities. Each of these Cloud Utilities will be responsible for maintaining their operations and sustainability.

As part of the initiative, a seed funding may be provided to Cloud Utilities to establish the respective cloud computing environments at the national level. However, for providing services (including services based IaaS, PaaS, SaaS and eGov AppStore) to the users and financial sustainability, they will have to evaluate the following options:

- **Own Development and Operation**: Cloud Utilities will have to select a system integrator (SI) for constructing the cloud computing environment. However, these Cloud Utilities will operate and maintain their respective cloud environments and market their cloud services on their own or through an agency with their own investments.

- **PPP Option**: The cloud computing environment will have to be set up by the SI. The SI will operate and maintain the operations for a specific period of time. The capital and operational investments will be shared between the Cloud Utility and the SI (the private partner) on agreed terms and conditions. They will also share revenue generated from provisioning of cloud computing services.

State Clouds

As a part of the SDC scheme of the government, the existing SDCs are being augmented with cloud infrastructure in a limited way. Some of the options listed below were explored for setting up, operating, maintaining and marketing the cloud services for the SDCs.

Option 1:

a. Private Cloud Service Provider in SDC for supply, installation testing and operations of the Cloud.

A private cloud service provider or operator can be selected using a competitive bidding or RFP process for implementing the cloud infrastructure at SDC. The service provider or operator can leverage the existing physical space and non-IT infrastructure of SDC. IT procurement for cloud implementation will be done by the selected cloud service provider.

However there are a few concerns in this business model and they are as follows:

- Since SDC might be operated and maintained by a Data Centre Operator (DCO) selection of a private cloud service provider would be a major concern. To prevent this, it may be possible that existing DCO is not selected as a L1 bidder for cloud implementation.

- DCO's consent might be required and a tripartite agreement will need to be established between the state nodal agency, DCO and the new cloud service provider for the following:
- Providing information about current SDC set up (system documentation, network architecture, etc.)
- Access to SDC infrastructure (for e.g. network device access, BMS components)
- Other implementation support activities
- Monitoring and review of the SLAs (for uptime, problem resolution, etc.) for both the service providers would be a concern as well. Nodal Agency as a Cloud service provider in SDC

b. Private Cloud Service Provider in SDC for supply and installation of the Cloud and operations of the SDC with the DCO

A private cloud service provider or operator can be selected using a competitive bidding or RFP process for supply and implementation of the cloud infrastructure at SDC. The service provider/operator can leverage the existing physical space and non-IT infrastructure of SDC. IT procurement for cloud implementation will be done by the selected cloud service provider.

DCO will take over the cloud operations along with the management of the existing SDC operations after successful installation and acceptance done by the private cloud service provider.

Option 2: State's nodal agency can take a lead and act as a cloud service provider

This model is best suited for the nodal agencies having the following:

- Sufficient funds to aid future capacity planning and procurement of infrastructure to support the cloud environment
- Highly skilled composite team working in coordination with the DCO to provide the required support

Agreements and SLAs need to be established directly between the State nodal agency and OEMs for support activities, providing training to composite team, DCO staff etc. The nodal agency can provide IaaS, PaaS and SaaS.

Option 3: National or Other State SDC acts as Cloud service provider

In this business model, an SDC can leverage the services of other cloud service providers in the GI Cloud eco-system. This can be used for the following:

1. Sharing common applications (e.g. Maharashtra has offered Gujarat its UID enrolment Survey App (Android tablet based), along with customised reporting system, from its SDC
2. In situations to set up disaster recovery (DR) capabilities for critical applications
3. Scaling of Infrastructure
4. Remote Infrastructure management of the SDC by the National Cloud

7.2 Procurement Norms

In the current scenario ICT procurement is done either through issue of tender or through empanelment of OEMs. The tender can be an open or closed bid selection process based on the prevailing norms and financial rules, whereas empanelment of OEMs is done through government agencies like NICSI or DGS&D in accordance with financial rules. The ICT infrastructure procured using either of the two methods mentioned above is mostly a one-time procurement of hardware. Such procurement cycle takes three months to one year to complete. Adoption of cloud will transform the government's ICT portfolio because it will allow the government departments and agencies to purchase a broad range of ICT services in a utility based model. As a result, they will have to focus their effort on ICT operational expenditures (opex) and only pay for ICT services consumed instead of periodic capital expenditure (capex). This is different from the traditional mode of procurement where the focus is on a one-time hardware-centric procurement of ICT infrastructure.

Effective ICT procurement in a cloud computing model can help the government departments and agencies increase operational efficiencies, optimise resource utilisation, and adopt innovation across its ICT portfolio. This will help them deliver better and faster services to citizens. However, the present ICT procurement guidelines are aligned towards the traditional model. With the adoption of cloud computing the ICT procurement guidelines or norms will need to be defined to establish a faster access to the services without lengthy government procurement process.

It is recommended that the Cloud Utilities release a defined rate card that is accessible to the departments. They can also empanel their service rate cards with the government agencies like NICSI, DGS&D to provide a ready reference and easy procurement as per the government norms. However, a detailed study on the need for amendment of procurement norms needs to be done in partnership with agencies as well as Department of Expenditure and the Finance Ministry. A reference rate card along with a case study has been provided in annexure 'IV'.

8 Implementation

8.1 Implementation Principles

The Implementation Strategy revolves around four principles shown below:

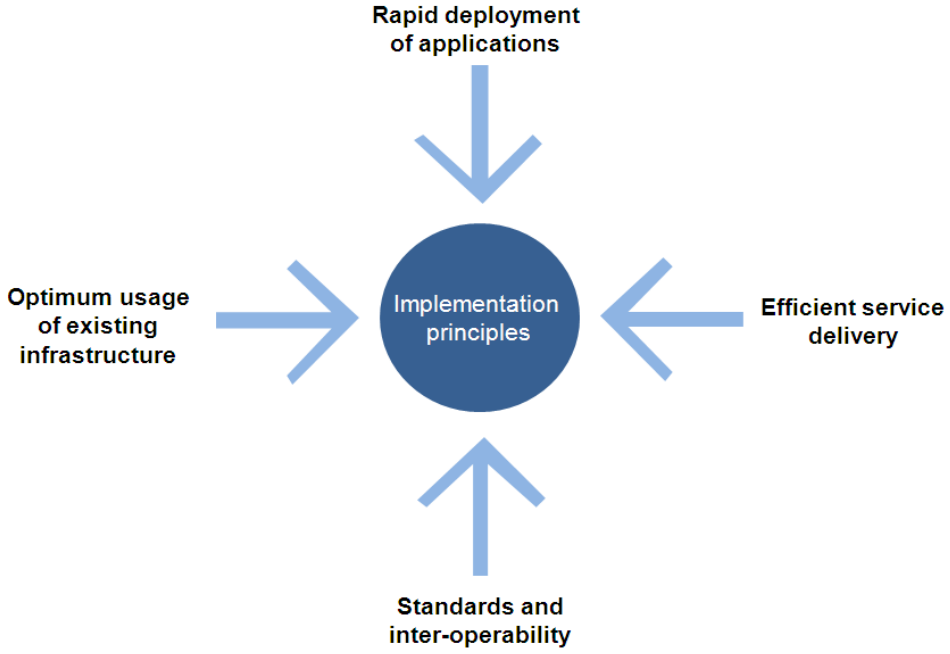


Figure 6: GI Cloud implementation principles

a) **Optimum usage of existing infrastructure:** As identified in the section under assessment of present infrastructure, there is already a huge investment for the creation of e-government services under the various national and state projects. The efficient utilisation of this invested infrastructure is the foremost priority while envisioning creation of a GI Cloud.

b) **Rapid deployment of applications:** There's a long gestation cycle of procurement of infrastructure, application development, testing and deployment for most e-government projects. The GI Cloud environment on the other hand, will provide the requisite platform for faster deployment of applications as infrastructure and platform can be procured as service. The GI Cloud having AppStore facility will also provide some applications which are ready to be customised and deployed as per the user requirements. This will essentially bring down the overall time required for development and deployment of applications.

c) **Efficient service delivery:** GI Cloud will ensure optimal utilisation of resources, infrastructure and speedy deployment of applications. However, the expected end result is efficient delivery of services through its faster availability.

d) **Standards and inter-operability:** The envisaged GI Cloud environment consists of NDCs and SDCs interconnected by a network backbone creating a secured, on-demand space of technology, platform, infrastructure and services for the government. For effective implementation, the same standards will need to be defined for security, network, storage, technology, governance, compliance, inter-operability and data portability.

8.2 Decision Criteria for Implementation Prioritising

The list of strategic initiatives identified for GI Cloud in the previous section needs to be prioritised to help determine what should get delivered or implemented first for establishment of the GI Cloud. Below are the lists of parameters identified for prioritising:

- Time to deliver
- Value of outcome
- Manageability of risk to business operations
- Achievability of the plans for implementation
- Roles and responsibilities of stakeholders
- Interdependence and dependency on other initiatives.

8.3 Prioritising and Sequencing Strategic Initiatives

In addition to the list of strategic initiatives for which funding may be provisioned by DeitY, there are other activities which need to be completed in order to establish the GI Cloud eco-system. These include approval of the cloud policy and implementation strategy for GI Cloud, establishment of the Empowered Committee for GI Cloud under the Chairmanship of the IT Secretary, DeitY, creation of AMO and CMO under DeitY.

Phase I: Strategy and Policy Establishment

Step 1: Approval of the policy and proposed strategy for GI Cloud

Phase II: Implementation

Step 2: Establishment of the Empowered Committee for GI Cloud to provide strategic guidance to DeitY and other stakeholders for the entire GI Cloud initiative

Step 3: Establishment of GI Cloud Expert Group

Step 4: Government agency to initiate the National Cloud, National eGov AppStore and National e-Services Directory establishment process

Step 5: Establishment of CoE including AMO

Step 6: Set up of CMO to assist DeitY in co-ordination, management and monitoring of the entire GI Cloud initiative

Step 7: DeitY to conduct study for demand assessment, application sensitivity and data profiling across Government departments in centre and states

Step 8: DeitY/national Government agency to publish various guidelines and standards security, application development and productisation, service delivery, operational aspects, contract management, procurement, tariff and pricing and template RFPs for cloud. This activity may be done by AMO

Step 9: DeitY to initiate the establishment process for the Cloud Utilities

Step 10: Set up the other clouds at the National level and the respective eGov AppStores

Phase III: Monitoring, management and ongoing improvement

Step 11: Design, implement, monitor and review of the overall GI Cloud program

Step 12: Incorporate suitable modifications as per learning or change requirements

8.4 Envisaged Risks, Challenges and Dependencies during Implementation

Some of the risks / challenges envisaged during the adoption of cloud computing by government are listed below:

- Security, interoperability issues in cloud may also act as a hindrance towards cloud adoption
- Legacy applications having complex architecture which involve high effort and monetary investment for making them cloud ready
- Availability of technical competency to manage the cloud environment
- Alignment of traditional procurement norms for cloud
- Awareness and change of mindset of user departments for cloud buy-in

Through the various initiatives being taken by the government within GI Cloud, it is expected that the government will be able to address these concerns.

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.

9 Annexure I: Snapshot current Government ICT infrastructure

National Data Centres

The National Informatics Centre (NIC), under the Department of Electronics and Information Technology (DeitY) has set up National Data Centres (NDCs) at Delhi, Hyderabad and Pune which provide shared hosting and co-location facilities to the government across India. Besides this, mini data centres are also operational in all NIC state centres to cater to the e-governance requirements at the State level. All the NDCs also act as disaster recovery (DR) site for State Date Centres and some organisations.

The National Data Centre at Pune built over 10,000 square feet was commissioned in March 2010 and is now fully operational, having 137 server racks and 400 TB of storage. The centre offers a virtualised environment for hosting application systems.

National Data Centre at Hyderabad acts as a DR site for NDC, Delhi and some of the state centres, apart from hosting large number of critical applications. It is also the DR site for the messaging services offered by NIC. The data centre has around 600TB of storage available for these services.

NIC has recently set up a state of the art tier-III data centre at Delhi to provide services to various e-governance initiatives undertaken by the government. The centre is built over an area of 60,000 sq. ft. and has over 480 racks. NIC is now in the process of setting up a data centre over 20,000 sq ft at Bhubaneswar. NKN acts as the backbone for connectivity for these NDCs.

Some of the important e-governance applications and services being delivered from the NDCs are Passport Information System, e-Post, Speed Post, NDNC Registry, Transport, Excise, Pension, Land Records, National ID, Utility Mapping, The NDCs are protected by multi-tier security infrastructure to extend optimum level of security to the government information and services.

State Data Centres

The State Data Centre (SDC) scheme under NeGP was approved by the Government in 2008 with funding from the central government. States were categorised into three categories large, medium and small. The aim of the scheme was to create a 'seamless secured infrastructure' deployed at the states and union territory headquarters. Total ownership was vested in the state governments and was used for delivery of various G2G and G2C services.

At present, SDCs in 19 States are operational (Gujarat, Tripura, Rajasthan, West Bengal, Tamil Nadu, Puducherry, Andhra Pradesh, Meghalaya, Karnataka, Manipur, Orissa, Sikkim, Haryana, Kerala, Maharashtra, Nagaland, Uttar Pradesh, Andaman and Nicobar and Madhya Pradesh). SDCs in six States are under implementation (Jharkhand, Chhattisgarh, Madhya Pradesh, Lakshadweep, Mizoram, and Jammu and Kashmir). Currently in about nine of these SDCs, the utilisation of infrastructure has reached 50%. The 19 State Data Centres are running a good number of applications such as commercial tax, e-Procurement, Bhoomi, mandi board etc. Line departments of these states are happy to get the reliable and secure services from the SDCs.

Different service models are being provided from the SDCs, such as the following:

- Collocations Services: Where the departments can bring their own infrastructure and applications and host them in a SDC. They get the core services from SDC such as power, cooling, rack space, internet, network and security.
- Shared Services: The departments bring their applications and host them on the infrastructure provided at SDC under the SDC Scheme.
- Managed Services: These services can be combined with any of the two services above, and it also includes L1 support, backup, storage, antivirus, helpdesk, etc.

SDCs have been equipped with infrastructure which will enable respective state and union territory departments with seamless, highly reliable, robust, shared and secured infrastructure with scalable capacity.

State Wide Area Networks

State Wide Area Network (SWAN) is one of the three core infrastructure components of the National e-Governance Plan (NeGP), which was designed to establish wide area network across the 35 states and union territories so that a common secure IT

infrastructure is created to enable seamless delivery of government to government (G2G), government to citizen (G2C) and government to business (G2B) services.

SWAN is envisaged as the converged backbone network for data, voice and video communications throughout a state or union territory and is expected to cater to the information communication requirement of all the departments right down to the block level.

At present the SWANs in 30 states (Andhra Pradesh, Chandigarh, Chhattisgarh, Delhi, Gujarat, Goa, Haryana, Himachal Pradesh, Jharkhand, Kerala, Karnataka, Lakshadweep, Maharashtra, Orissa, Punjab, Puducherry, Sikkim, Tamil Nadu, Tripura, Uttar Pradesh, West Bengal, Assam, Bihar, Madhya Pradesh, Uttarakhand, Manipur, Arunachal Pradesh, Meghalaya, Nagaland and Mizoram) are operational. The SWAN in Rajasthan is in advance stage of implementation. Jammu and Kashmir have initiated the bid process to identify the network operator for implementation. Dadra and Nagar Haveli and Daman and Diu are in RFP and BOM finalisation stage.

Presently all the State Head Quarters (SHQs) and District Headquarters (DHQs) are connected on fibre (barring few DHQ's). It is envisaged that all the Block Headquarters (BHQs) will also be connected through fibre in due course of time. The network of SWAN is created using MLLN and non- MLLN Circuits. They will now be transformed in to MPLS circuits. For remote horizontal offices the option of wireless connectivity is also being explored.

National Knowledge Network

National Knowledge Network (NKN) is a state-of-the-art multi-gigabit pan-India network for providing a unified high speed network backbone for all knowledge related institutions in the country. Together with the NICNET, it is acting as the e-governance backbone of the country. All NDCs are connected through NKN and NICNET and now SDCs and SWANs are in the process of being integrated through this network.

Initial phase has been successfully executed by the National Informatics Centre (NIC). The architecture of NKN has been designed for reliability, availability and scalability.

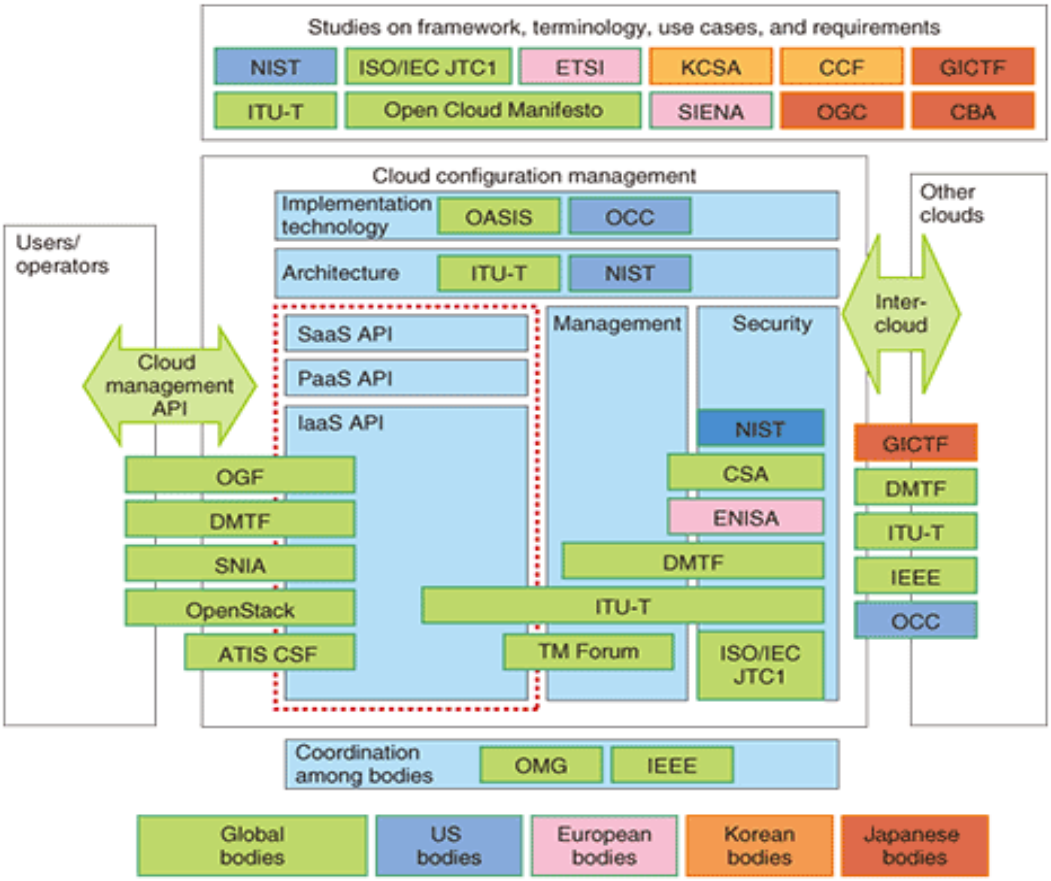
National Optical Fibre Network

The Department of Telecommunications (DoT) in 2011 cleared creation of a National Optical Fibre Network (NOFN) that would provide broadband connectivity to all village panchayats (2,50,000 in number) in three years. The plan is to extend the existing optical fibre network initially up to the panchayats and then create an institutional mechanism for management and operation of the NOFN for ensuring non-discriminatory access to all service providers. The project is being funded through the Universal Service Obligation Fund (USOF). The project is to be completed by 2014-15 through a SPV called Bharat Broadband Network Ltd (BBNL).

NFON will also help the government implement its various e-governance initiatives such as e-health, e-banking and e-education, facilitating inclusive growth. NOFN will enable effective and faster implementation of various mission mode e-governance projects as well as delivery of a whole range of electronic services by the private sector to citizens in rural areas.

10 Annexure II: Standards

Since cloud computing involves a wide range of technical and business elements, the targets of cloud computing standardisation are diverse and many organisations are studying cloud computing standards focussed on their respective areas of expertise. The different study areas and major cloud computing standards bodies related to each of them are shown in figure below.



OGC: Open Government Cloud consortium
CBA: Cloud Business Alliance
SIENA: Standards and Interoperability for e-infrastructure Implementation initiative
KCSA: Korea Cloud Service Association
ATIS CSF: Alliance for Telecommunications Industry Solutions Cloud Services Forum

Figure 7: Study areas for cloud computing standardisation and major cloud computing standards bodies (Source: Standardisation activities for cloud computing, NTT)

11 Annexure III: Illustrative Evaluation Criteria for Hosting Applications on eGov AppStore

S. No.	Weightage	Criteria	Sub-criteria
1	High	Core configurability and customisability	The core functionality of the application is generic, exhaustive and meets the requirements
			Configurable for adaption in other states
			Time and cost to customise
2	Medium	Architectural upgradeability and flexibility	Does the application follow centralised architecture and multi-layered architecture pattern
3	Medium	Technology used for building the solution	Does the technology need up-gradation (i.e. database and OS)
			Technology used and the cost of the solution with breakup
			Cost and time for migrating the technology (e.g. database, application server, OS, etc.)
4	High	Deployment location and cost of the solution	Dedicated hosting in own state SDC or NDC or remote SDC
5	High	Capability to scale up and total transactions	No. of concurrent users served
			No. of concurrent users it can serve (stress test)
			No. of transactions per minute
			Total transactions served during peak / average times
			How many transactions has the application handled till date
			Response time (peak / average times)
6	High	Security	Is the application security certified
			Have security features been in built in the application (in case if not certified)
7	High	IPR (de jure and de facto)	Is the IPR with the government
			is the source code available
			Is the documentation available
			Does the govt. / govt. agency has in-house capability for customisation and maintainability
8	High	Multi-tenancy	Does the application follow a multi-tenant architectural platform
			Can the application be made multi-tenant
9	Low	User interface and language	Can the application be used a web-service
			Does the application support more than one language

12 Annexure IV: Case Study – Government of Maharashtra

Maharashtra state along with MahaOnline is providing various categories of services through cloud implemented in Maharashtra State Data Centre (SDC). The categories of services provided by SETU Maharashtra in SDC using cloud are following:

1. Infrastructure as a Service (IaaS)
2. Platform as a Service (PaaS)
3. Software as a Service (SaaS)
4. Miscellaneous Services

Apart from services provided by SDC, MahaOnline is also providing various services as below:

- Software as a Service (SaaS)
- BI as a Service (BIaaS)
- GIS as a Service (GISaaS)
- API as a Service (APIaaS)
- Survey as a Service (SyaaS)

The following terms will be applicable for all the services provided by SETU Maharashtra and MahaOnline:

- Departments may place the order on SETU or MahaOnline.
- Any of the services of SETU can be provided by MahaOnline and vice-versa at the rates mentioned above
- Internally, SETU and MOL can offload some items to each other
- The rates will be revised from time to time
- Service tax will be applicable on all the services

A rate card has been developed by the Government of Maharashtra and is publicly available at maharashtra.gov.in under the rate contracts category (https://www.maharashtra.gov.in/Site/Common/RateContract.aspx)

13 Annexure V: 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)
- Directorate of Information Technology, the Government of Maharashtra
- Centre for e-Governance, the 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

14 References

- NeGP website - http://www.negp.gov.in
- NISG website – http://www.nisg.org
- National Informatics Centre Annual Report 2011
- Guidelines for application productisation and roll-out prepared by DeitY
- Electronics and Information Technology Annual Report, 2011-12
- Data Centre Strategy, G-Cloud & Applications Store for Government Programme
- NIST Cloud Computing Reference Architecture, Special Publication 500-292
- NIST Cloud Computing Standards Roadmap, Special Publication 500-291