E-Government and e-Governance:

E-Government Definition:

E-Government refers to the implementation of information and communication technology (ICT) like internet, to improve government activities and process. E-Government aims of increasing transparency, efficiency and citizen involvement in the various government schemes, operations and process. Hence it speeds up the justice delivery system in the country.
Government may be defined as the integration of information and communication technology, in public administration, i.e. to various government processes, operations, and structures with the purpose of enhancing transparency, efficiency, accountability and citizen participation.

Benefits of e-Government

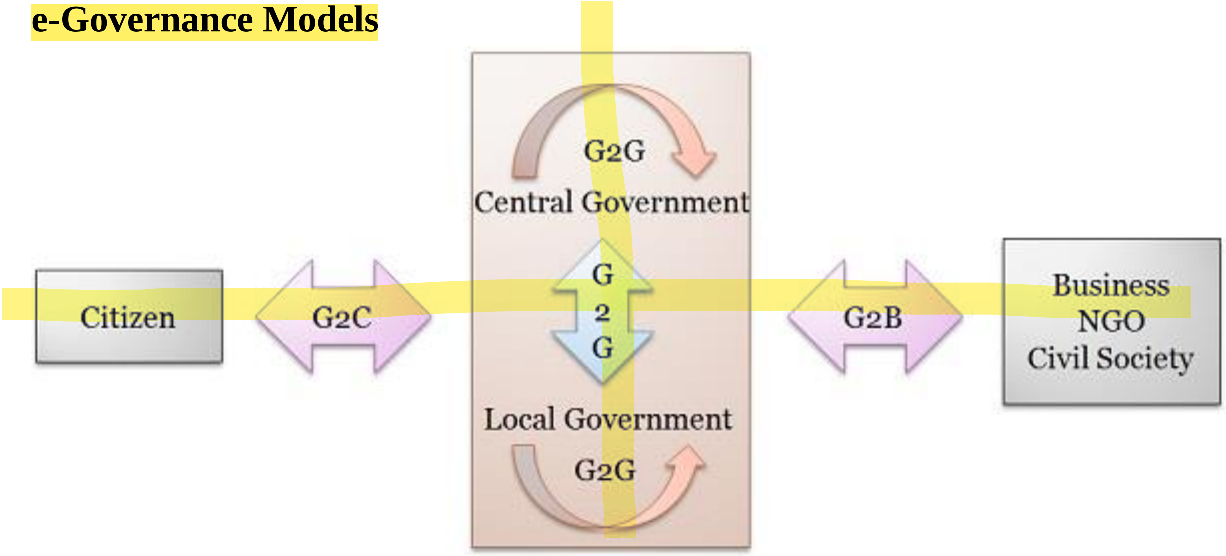
1. It ensures greater level of efficiency and effectiveness in government activities and operations.
2. Improves access of information to the common mass.
3. It ensures the transparency in the operation of government programmers.
4. It increases the reach of the government to the general public
5. It helps in improving the quality of public services
6. Increases communication between various government agencies.

E-Governance Definition:

Electronic governance, shortly known as e-governance refers to the utilization of information and communication technology (ICT) for **providing** government services, disseminating (broadcasting) information, communication operations with the general public.
Electronic governance or e-governance is the application of information and communication technology (ICT) for delivering government services, exchange of information communication transactions, integration of various stand-alone systems and services between government-to-customer (G2C), government-to-business (G2B), government-to-government (G2G) as well as back office processes and interactions within the entire government framework.
In simple words, e-Governance enables public in availing services, operations, schemes with the help of information and communication technology (ICT).
E-governance is a tool, that makes available various government services to citizens in a convenient way, such as:

- Better provision of government services
- Improved interaction with different groups
- Citizen empowerment through access to information
- Efficient government management

e-Governance Models



e-Governance Model

- **G2G (Government to Government):** The exchange of information between government agencies or departments, i.e. within the confines of government is called as G2G interaction.
- **G2C (Government to Citizen):** As the name suggests, it is the interaction between government and the citizens of the country. It involves establishing an interface, to enable the general public to access information and services, whenever and wherever they want. They can also give their feedback with respect to policies and rules.
- **G2B (Government to Business)**: The dissemination of information between government and the business, is G2B interaction. It focuses on reducing red-tapism, establishing transparency and accountability in the business environment.
- **G2E (Government to Employees):** The interaction between government and employees to increase employee morale and satisfaction, is made easier and faster with the help of information and communication technology.

Objectives of E-Governance

The object of E-Governance is to provide a SMARRT Government. The Acronym SMART refers to Simple, Moral, Accountable, Responsive, Responsible and Transparent Government.

- S – The use of ICT brings simplicity in governance through electronic documentation, online submission, online service delivery, etc.
- M – It brings Morality to governance as immoralities like bribing; red-tapism, etc. are eliminated.
- A – It makes the Government accountable as all the data and information of Government is available online for consideration of every citizen, the NGOs and the media.
- R – Due to reduced paperwork and increased communication speeds and decreased communication time, the Government agencies become responsive.

- R – Technology can help convert an irresponsible Government Responsible. Increased access to information makes more informed citizens. And these empowered citizens make a responsible Government.
- T – With increased morality, online availability of information and reduced red-tapism the process of governance becomes transparent leaving no room for the Government to conceal any information from the citizens.

Advantages of E-Governance

The e-governance is becoming a celebrated concept and the sole reasons are the advantage which it brings with it in the country it is applied. The advantages if ICT are many and "the use of information and communications technologies (ICT) to improve the efficiency, effectiveness, transparency and accountability of government" .

1. **Reduces the cost**

   This is a significant achievement which an e-governance scheme procures, as we know that most of the Government expenditure is appropriated towards the cost of stationary and paper works. This Paper-based communication proves to be a costlier one and this sucks in a lot of governments or public money as it calls for constant heavy expenditure. The solution to this problem is this electronic way of working, Internet and Phones makes communication cheaper saving valuable money for the Government.
2. **Speedy working**

   E-governance works on the basis of Technology and it is a known fact that technology makes communication speedier thus this is what makes the working speedier and the working becomes faster. Internet, Phones, Cell Phones have reduced the time taken in normal communication.
3. **Increase Transparency**

   The main concern of any nation in the present era is the increasing and continuing corruption in the system. This can also be solved through the use of ICT which makes governing profess transparent. All the information of the Government would be made available on the internet and right to information of citizens would be taken care of and respected. This revolutionizes the way governments function, ensuring much more transparency in the functioning, thereby eliminating corruption. The citizens can see the information whenever they want to see and ICT helps the citizen in this aspect and leaves no way in which the information could be concealed from the citizens and therefore it helps in reducing corruption and in a way it makes the governance more transparent.
4. **It brings Accountability**

   When the governing process is made transparent the Government automatically becomes accountable and accountability is a very basic requirement of good governance. Accountability includes answerability of the Government to the people about its working and this is right of the people to know exactly about the functioning of the government. E-governance therefore makes a noteworthy contribution in the society by providing a better government which is accountable to its citizens and this fulfills the basic requirement of the demand of the population which elects its government.

Challenges In The E-Governance:

E-governance is a constructive idea that can be of an immense positive output but it is not so easy to attain in a country like India which is practically a developing nation. E-governance itself is a very technical scheme and it has challenges which make the implementation easier said than done.

The most significant characteristic of any successful e-government application is its quality (Signore, et al 2005) and accessibility. The issue (Cost, Time) of integration of legacy systems comes onto the scene. As the information collected by governments may be politically sensitive, installation of appropriate security mechanisms may be an important technical consideration. At the same time, many other policy issues need to be resolved, such as authentication and confidentiality.

1. **Digital Divide**

   The digital divide refers to the separation that exists between individuals, communities, and businesses that have access to information technology and those that do not have such access. Social, economic, infrastructural and ethno-linguistic indicators provide explanations for the presence of the digital divide. Economic poverty is closely related to limited information technology resources. An individual living below poverty line does not afford a computer for him to harness the benefits of e-government and other online services. As the digital divide narrows, broader adoption of e-government in the public domain becomes possible. E-governance is totally based on modern technology and it will be a failure if this part is not taken into consideration. Technology has to be in the reach of the people for whom the policies are made and who have to use them.

2. **Lack of communication**

   India is a country which has decentralized government and in such a case the power is decentralized and does not only rest in the hands of centre but divided in different spheres and departments, so the lack of communication between these departments is one of the biggest challenge that India has to face while opting for E-governance. So the information that exists in one department has no or very little use with respect to some other department of the government.

3. **Population**

   This comes out to be probably biggest challenge for the e-governance. E-governance requires huge amount of work for making the databases of the citizens of the country and doing it efficiently for such a population is in itself a very big task. Security issues and privacy issues are also to be dealt with proper care and so it becomes a little hindrance.

4. **Different Languages**

   In a country like India which is highly diverse, language comes as a barrier in the path of communication and this is a very important expect of success of the any scheme. Ensuring E-

Governance in local language is a big task to achieve. Supplying information to the public in a language that they understand and are comfortable with, and generally, it is the local language. As, technology is available by which transliteration from English into other languages can be made. Therefore, the problem is manageable provided there is enough motivation to do this onerous task.

Key Differences between e-Government and e-Governance

1. By e-Government we mean the use of ICT in government operations, as a tool to increase the outreach of the government services. E-Governance, on the other hand, implies the use of ICT in transforming and supporting functions and structures of the system.
2. e-Government is a system while e-Governance is a function.
3. e-Government is a one-way communication protocol. On the contrary, e-Governance is a two-way communication protocol.

e-Government as information systems:

e-Government is the use of IT by public sector organizations. To understand e-government, we must therefore understand IT. What does IT do: it handles data to produce information. The next step to understanding e-government, then, is to understand that e-government systems are information systems. A system is a collection of elements that works and has a purpose. To understand e-government as an information system, we must add in some notion of activity and purpose.

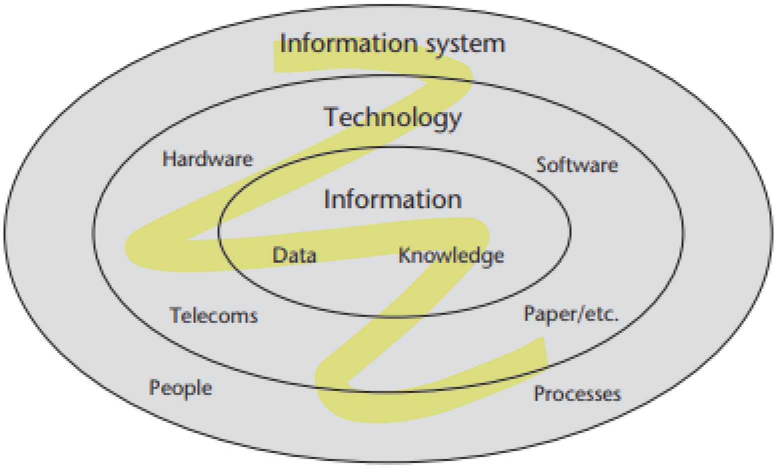


Figure 1.1 eGovernment systems as information systems: Structural view

Figure 1.1 shows e-government systems can be described as ‘socio-technical systems’ because they combine both the social – that is, people – and the technical. his is a first indication that, when managing e-government, both social and technical (otherwise known as soft and hard) issues will have to be dealt with.

The ITPOSMO Checklist

ITPOSMO checklist can be used for describing and understanding any e-government system and stakeholder organizational context.

- Information: The formal information held by the digital system and the informal information used by the people involved with the system.
- Technology: Mainly focuses on digital IT but can also cover other information handling technologies such as paper or analogue telephones.
- Processes: The activities undertaken by the relevant stakeholders for whom the e-government system operates, both information-related processes and broader business processes.
- Objectives and values: Often the most important dimension since the objectives component covers issues of self-interest and organizational politics, and can even be seen to incorporate formal organizational strategies; the values component covers culture: what stakeholders feel are the right and wrong ways to do things.
- Staffing and skills: Covers the number of staff involved with the e-government system, and the competencies of those staff and other users.
- Management systems and structures: The overall management systems required to organize operation and use of the e-government system, plus the way in which stakeholder agencies/groups are structured, both formally and informally.
- Other resources: Principally, the time and money required to implement and operate the e-government system.

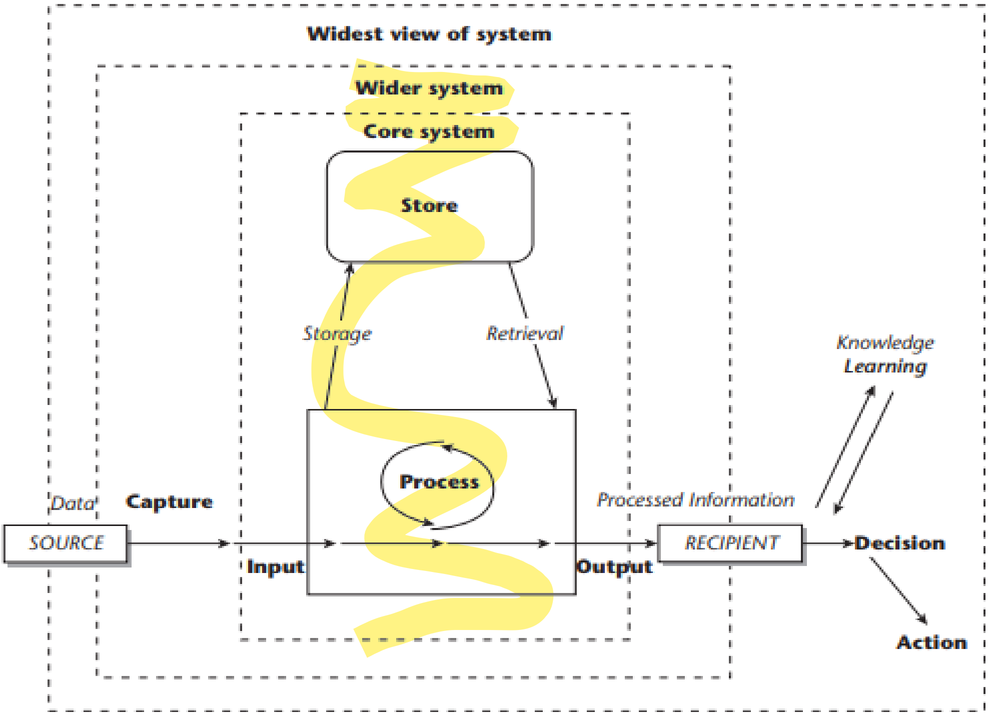


Figure 1.3 eGovernment systems as information systems: Process view

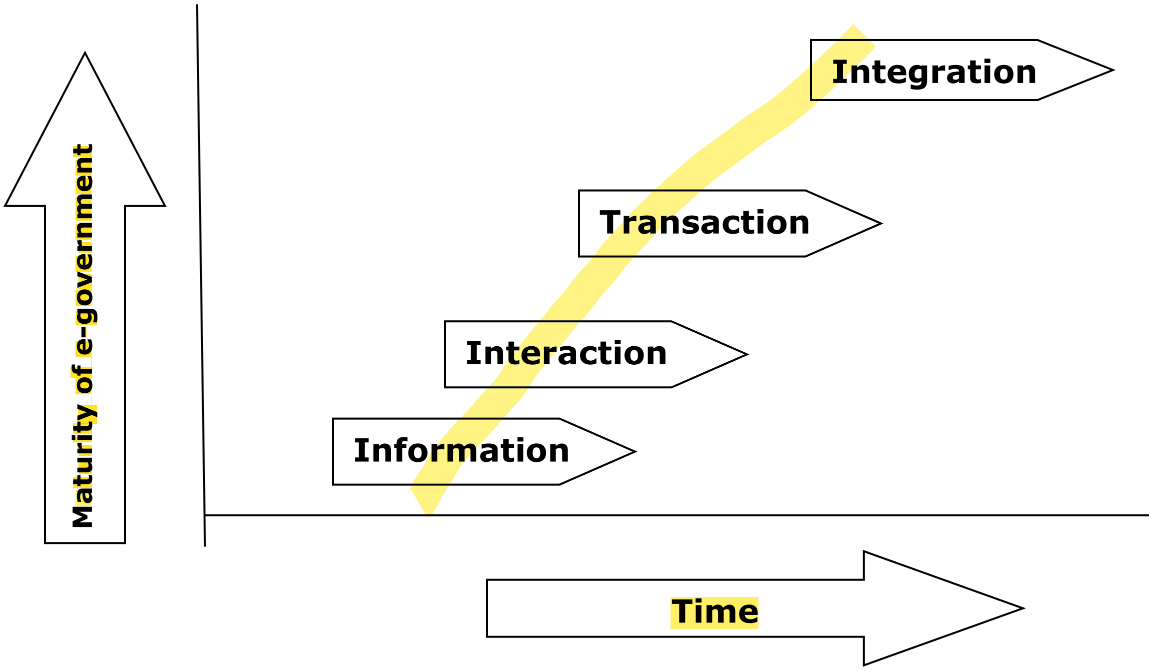
The CIPSODA Checklist:

This understands an e-government application in terms of its information-related tasks: a process view to go alongside the structural view.

CIPSODA checklist, illustrated in Figure 1.3. The checklist of tasks can be explained in some further detail, using the example of part of an e-tax system:

- Capture: Gathering the raw data necessary for the e-government system. The taxpayer obtains the basic data on their various sources of income.
- Input: Entering the data onto the system. The taxpayer types the data into an e-form on the revenue agency's web site.
- Process: Altering the data via calculation, classification, selection, and so on. The e-tax system uses the different tax rates for different income types to calculate the total tax owed.
- Store: Holding raw and processed data on the system. The e-tax system stores all details entered and calculated about this taxpayer.
- Output: Issuing the processed data. The total tax calculated is displayed to the taxpayer.
- Decision: If the processed data is useful enough to be seen as information, it is used for decision making. The taxpayer determines whether to challenge or accept the calculated tax sum.
- Action: Implementation of the decision. If all is well, the taxpayer authorizes payment of the tax owed.

E-government stages of development



There are four stages of e-government development

i. **Information**: This is the initial stage of web presence. A few web sites are launched that contain limited and static information, which is updated more frequently with increasing usage and customer pressure. The information may be limited to the basic functions, facts and figures and contact details of government departments and agencies. The information stage does not call for any efforts at 'computerization' of the backend. The information web sites of this type can be set up typically in 4-6 weeks.

ii. **Interaction**: In this stage, the citizens can 'interact' with government agencies in a 'one-way street' manner. The citizens can download forms, file forms, returns and complaints online, with government agencies. The capacity to search specialized databases and send e-mails to government agencies and links between related web sites are also available. This stage calls for building capacity and systems in the backend government agencies to receive the requests sent by the citizens online and to process the same in sequential and accountable manner.

iii. **Transaction**: This is a much more difficult stage to reach. In this stage, the citizens can go through a full cycle of fulfillment of their requests. It is a two-way street. Complete and secure transactions such as online payments for utility bills, taxes, fees, registrations, renewals, obtaining permits, licenses and certificates are typical examples of interactions. E-procurement, online customs clearances, single window and single-sign-on are more sophisticated examples of this stage.

iv. **Integration**: This stage visualizes offering government information and services in an integrated manner- integrated not from the government's point of view but from the citizen of business' viewpoint. A very useful way of envisioning this stage is to package the information and services around the key events in the life cycle of a citizen or business. The key events in a citizen's life are – birth, admission to school, admission to college/university, employment, housing, marriage, shifting of job/house, Medicare, senior citizenship and death. The key events in the business life cycle are – registration of a firm/company, securing all clearances for setting up business/industry, filling of returns, payment of taxes and so on.

Online Service Delivery and Electronic Service Delivery

This is, by far, the most visible impact of e-government to the extent that, often, e-government is identified with provision of electronic services. Electronic service Delivery (ESD) is obviously beneficial to the citizen and other customers of the government in a variety of ways. But what are the benefits to the government itself in ESD?

a. **Better Image**: speed, efficiency, transparency and convenience arising out of ESD enhance the image of government. This is in fact one of the strongest factors driving governments all over the world towards e-government.

   Theoretically, e-government can result in significant cost reduction. This premise rests on the belief that the automation of processes reduces manpower costs, besides costs of accounting, compilation, reporting and review.

b. **Better targeting of benefits**: E-government projects in the social sectors, especially in the areas of welfare, health and education in the context of developing countries, bring in the benefits arising out of better targeting of benefits schemes. Electronic databases of citizens, employees and establishments, use of electronic identity cards, coupled with powerful search tools, named-based systems and the like, result in identification of the most deserving beneficiaries among the target group, and reduce the scope for duplication of benefits to the same individual or for drawing of benefits in the name of fictitious persons and institutions. E-government can enhance the effectiveness of welfare programs and prevent frauds and leakages.

c. **Control of Corruption**: The speed, transparency and accountability brought into government agencies, coupled with the simplification and rationalization of procedures as a part of e-government, create an environment that discourages corrupt practices or in the least makes it easier to detect them and punish the culprit.

2

Public –Private partnership:

PPP is a mode of providing public infrastructure and services by Government in partnership with private sector. It is a long term arrangement between Government and private sector entity for provision of public utilities and services.

A PPP project means a project based on a contract or concession agreement between a Government and a private sector company for delivering a government service on payment of user charge.

So, A Public-Private Partnership in e-Government may be defined as a legally enforceable contract between a private sector entity and a government body that requires the private partner to deliver a desired electronic public service, for which the private sector must invest some of its own resources (financial, technological, time, corporate reputation, etc.), and must become responsible for some of the risks of service delivery, and for which payments to the private partner are made only in exchange for actual performance delivered. Generally, the operating risks are allocated to the private sector partner (generally the "commercial" risks) while the "political" risks are allocated to the public sector partner.

Public-private partnerships allow large-scale government projects, such as roads, bridges, or hospitals, to be completed with private funding.

These partnerships work well when private sector technology and innovation combine with public sector incentives to complete work on time and within budget.

Risks for private enterprise include cost overruns, technical defects, and an inability to meet quality standards, while for public partners, agreed-upon usage fees may not be supported by demand—for example, for a toll road or a bridge.

The goals of PPPs in e-government are:

- To mobilize new private sector investment in order to leverage public funds required in the development of e-government networks, including both underlying information and communications technology infrastructure and equipment, as well as the public services being delivered on these networks;
- To attract private sector experience, technology, and innovation in the design of electronic networks and services, and to benefit from private sector creativeness and ingenuity; and
- To utilize private sector marketing channels and customer service expertise in the commercial delivery of services to customers of the e-government system.

Public–private partnership (PPP) has following main features:

- A long-term contract between a public sector authority and a private party.
- The private party provides a public service or infrastructure.
- Private party assumes substantial financial, technical and operational risk. There is well defined allocation of risk between the private sector and the public entity and the private entity receives performance linked payments that conform (or are

benchmarked) to specified and pre-determined performance standards, measurable by the public entity or its representative.

Significance to Government:

- Provides required capital while meeting public needs.
- Attracting private capital to fund public projects.
- Potential to improve the quality of service made available at lower costs.
- Sharing of financial load and risk.
- Development of local private sector capabilities in form of joint ventures and sub-contracting.
- Supplements limited public sector capacities.

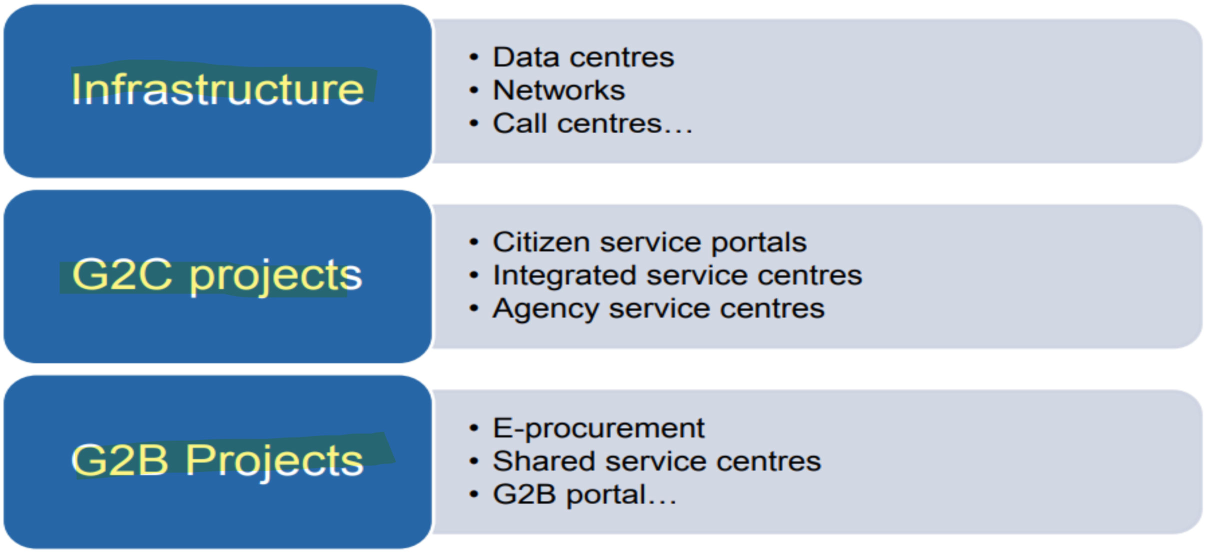
Significance to Private partner:

- Fund provides required gap capital while rest is met by private.
- Helps exposure to big scale projects and attract bigger foreign projects.
- Help to expand the span of quality service and operational efficiency.
- Sharing of financial load and risk and protection during market downturns.
- Contracts with Govt. help promote goodwill and opportunities of joint ventures and sub-contracting capabilities.

Why PPP for e-Government?

- The task is too large and complex for Government to execute-therefore partnerships are necessary
- Attract private resources. Government resources can be utilized for development infrastructure
- Private sector can bring project management and technical expertise lacking in the Government
- Private sector is better at interfacing with customers
- Partnerships force a certain discipline in project planning and execution.
- Entrepreneurship & local enterprise promotion
- Transformation means focus on core business of Government

Areas of PPP in e-Governance



Infrastructure

- Data centres
- Networks
- Call centres…

G2C projects

- Citizen service portals
- Integrated service centres
- Agency service centres

G2B Projects

- E-procurement
- Shared service centres
- G2B portal…

Forms/models of PPP:

PPP can be of different forms, depending on the shares of government and the private sector in the investment, control as also on the strategic nature and commercial viability of the project/initiative.

1. **JV Model**

   In this model, an SPV (Special Purpose Vehicle) is formed to undertake the e-government project and/or to provide e-services. The joint venture can be led by the government or by the private partner depending upon the strategic nature and sensitivity of the domain.

   A JV model is preferred for the following projects:

   a. delivering of services, which are basic and permanent in nature, e.g. a country portal,

   b. setting up of infrastructure with steady returns visualized in long term, e.g. State Data Centre,

   c. handling of sensitive data and information relating to citizens, businesses and government, e.g. DMV and

   d. Close coordination with and cooperation from a host of government agencies, e.g. Integrated Citizen Service Centers.

2. **BOO Model: Build-Own-Operate Model**

   In this model, the selected partner designs, develops and implements the project, most often, entirely at its cost and operates the system for a pre-specified period. The options of the partners are kept open till the end of the period- sometimes called the concession period. The revenue model of the project is either based on the transaction charges (paid by the citizen or the government) or on EQI/EMI (Equated

Quarterly Installment / Equated Monthly Installment) paid by the government to the operator/ service provider. The revenue model could also be a combination of a fixed EQI/EMI plus transaction charges.

The BOO model is suitable for projects that involve setting up of physical infrastructures such as service centre(s) for delivering services to citizens. Good examples are e-government projects relating to the issue of driving licenses, registration of vehicles, and provision of integrated services to citizen across the counter.

3. **BOOT (Build-Own-Operate-and-Transfer) Model**

   This is almost identical to the BOO model except that the government exercises the option to get the ownership of the assets created by the partner at the end of the project. The transfer cost is usually a small percentage- 5 to 10 % - of the initial capital cost of the project. The BOOT model is adopted where the technology is time-tested and the ICT assets are expected to outlast the concession period.

4. **ASP Model**

   The ASP (Application Service Provider) model is an example of PPP where the partnership is quite tenuous. In this model, the government contracts to avail the services of the partner for delivery of services as per mutually agreed service levels and commercial terms. The revenue model is typically transaction-based. The ASP model is suitable to e-government initiatives that involve

   a. a requirement to launch the services in a short time frame,
   b. the technology is not complex and is widely accepted and practices in the private sector, and
   c. the nature of information is not so sensitive or critical to governance.

   Examples of ASP model are

   i. design and hosting of websites that provide fairly static information to the citizens,
   ii. provision of simple services like downloading/filing of forms, and
   iii. provision of MIS services in the G2G arena to the government agencies.

   This creates a win-win situation by enabling the optimum utilization of the ICT infrastructure already set up in the private sector and thereby reducing the transaction cost to the government/citizen.

Issues in PPP for e-Government

i. **Lack of congruence in objectives:** PPP is about the partnership in realizing shared objectives. The various models in sharing the investment and controls are only organizational mechanisms. The success of PPP depends on the degree to which the public and private sector partners align themselves along these objectives. Failure to realize this certainly leads to failure of the venture.

ii. **Risk and Control:** Sharing of risk and control is another slippery area. Most often, governments attempt to transfer the risk to the partner without passing on the related controls to the partner quoting "public interest" as the reason. This results in one of the partners calling the shots and expecting the other partner to play the game.

iii. **Clash of cultures:** The organizational cultures of the private and public sector differ widely in all parts of the world. This is bound to result in conflicting situations. It is necessary to create a joint control and review mechanism that fosters mutual trust and confidence.

iv. **Monopoly:** Several of e-initiatives depend, for their viability, on the principles of aggregation of demand and economy of scale. Very often there is space for only one partner in areas such as e-procurement, country or state portal, data centre, gateway and the like. This is likely to result in a situation of monopoly- the monopoly of the state being replaced with the monopoly of the private partner and more importantly, monopoly of a particular technology.

Citizen-Centric Approach to e-Government

1. It is necessary to look at e-government from the citizen or customer's point of view and design the front-end and the back ends to the extent required to fulfill the requirement of citizen/customer. In other words, the e-government initiatives should not be system-driven or supply-driven but should be demand-driven.
2. The e-government projects can classified as core and non-core. Core projects are those that can be used by all departments across the state and with significant impact on key stakeholders like citizens, businesses and employees.
3. The e-government projects can also be categorized as commercial and non-commercial. Commercial projects are those that permit a viable public-private partnership model to be implemented with least outgo from public exchequer for implementation.

3

ICT Infrastructure for e-Government:

- A set of basic services and tools that enables the development and execution of electronic public services.
- It provides services that are typically used by many e-services.
- It is foundational and its usage spans several agencies.
- A platform for facilitating the interoperability of e-services.

Need of e-Government Infrastructure:

- growing number of offered e-services
- a web of relations emerging between e-services
- more agencies involved,
- more complex services
- increased level of sophistication and interactivity
- more users reached with more devices
- Industry taking over e-service development.

National E-Governance Infrastructure should primarily involve, setting up following facilities:

- Nationwide Communication Infrastructure/Network Infrastructure
- Computing Infrastructure
- Data Centers
- E-Government Architecture
- Interoperability Framework

Network Infrastructure:

While Communication Infrastructure needs to be setup for government to deliver its services online, there is an equally important need for setting up nationwide communication network for citizens to easily access government services whether in the urban areas or in the rural parts of the country.

Generally, urban parts of the country are already equipped with communication facilities.

Therefore, Government needs to pay more attention to the rural and remote areas of the country to avoid occurrence of another digital divide

Network Infrastructure is the platform that supports the network. It provides the stable and reliable channel over which our communications can occur.

The network infrastructure contains three categories of network components:

a. **End devices**
b. **Intermediary devices**
c. **Network media**

Devices and media are the physical elements, or *hardware*, of the network. Hardware comprises the components of the network platform that typically are visible, such as a laptop, PC, switch, router, wireless access point, or the cabling used to connect the devices. Occasionally, some network components may not be visible. In the case of wireless media, for example, messages are transmitted through the air using invisible radio frequency or infrared waves.

Network components are used to provide services and processes. These services and processes are the communication programs, called *software*, that run on the networked devices. A ***network service*** provides information in response to a request. Services include many of the common network applications people use every day, like email hosting services and web hosting services. Processes provide the functionality that directs and moves the messages through the network. Processes are less obvious to us but are critical to the operation of networks.

a. End Devices

The network devices that people are most familiar with are called ***end devices***, or hosts. These devices form the interface between users and the underlying communication network.

Some examples of end devices are

- Computers (work stations, laptops, file servers, web servers)
- Network printers
- VoIP phones
- Tele-Presence endpoints
- Security cameras
- Mobile handheld devices (such as smart phones, tablets, PDAs, and wireless debit/credit card readers and barcode scanners)

A ***host device*** is either the source or destination of a message transmitted over the network. In order to distinguish one host from another, each host on a network is identified by an address. When a host initiates communication, it uses the address of the destination host to specify where the message should be sent.

In modern networks, a host can act as a client, a server, or both. Software installed on the host determines which role it plays on the network. *Servers* are hosts that have software installed that enables them to provide information and services, like email or web pages, to other hosts on the network. *Clients* are hosts that have software installed that enables them to request and display the information obtained from the server.

b. Intermediary Devices

Intermediary devices interconnect end devices. These devices provide connectivity and work behind the scenes to ensure that data flows across the network. Intermediary devices connect the individual hosts to the network and can connect multiple individual networks to form an internetwork.

Examples of intermediary network devices are

- Network access devices (switches and wireless access points)
- Internetworking devices (routers)
- Security devices (firewalls)

The management of data as it flows through the network is also a role of the intermediary devices. These devices use the destination host address, in conjunction with information about the network interconnections, to determine the path that messages should take through the network.

Processes running on the intermediary network devices perform these functions:

- Regenerate and retransmit data signals
- Maintain information about which pathways exist through the network and internetwork
- Notify other devices of errors and communication failures
- Direct data along alternate pathways when there is a link failure
- Classify and direct messages
- Permit or deny the flow of data, based on security settings

c. Network Media

Communication across a network is carried on a ***medium***. The medium provides the channel over which the message travels from source to destination.

Modern networks primarily use the following three types of media to interconnect devices and to provide the pathway over which data can be transmitted:

- Metallic wires within cables
- Glass or plastic fibers (fiber-optic cable)
- Wireless transmission

The signal encoding that must occur for the message to be transmitted is different for each media type. On metallic wires, the data is encoded into electrical impulses that match specific patterns. Fiber-optic transmissions rely on pulses of light, within either infrared or visible light ranges. In wireless transmission, patterns of electromagnetic waves depict the various bit values.

Different types of network media have different features and benefits. Not all network media types have the same characteristics or are appropriate for the same purpose. The criteria for choosing network media are

- The distance the media can successfully carry a signal
- The environment in which the media is to be installed
- The amount of data and the speed at which it must be transmitted
- The cost of the media and installation

Computing Infrastructure:

Computing Infrastructure is another important dimension of National e-Government Infrastructure.

While on one end, government needs large computing infrastructure to develop and deliver e-government services on continuous basis, infrastructure is also needed at the end of citizens to derive the benefits of these services.

Computing Infrastructure refers to the composite hardware, software, network resources and services required for the existence, operation and management of an enterprise IT environment. It allows an organization to deliver IT solutions and services to its employees, partners and/or customers and is usually internal to an organization and deployed within owned facilities.

Typically, a standard Computing Infrastructure consists of the following **components**:

- **Hardware**: Servers, computers, data centers, switches, hubs and routers, etc.
- **Software**: Enterprise resource planning (ERP), customer relationship management (CRM), productivity applications and more.
- **Network**: Network enablement, Internet connectivity, firewall and security.
- **Meatware**: Human users, such as network administrators (NA), developers, designers and generic end users with access to any IT appliance or service are also part of an IT infrastructure, specifically with the advent of user-centric IT service development.

Data Centers:

– In the era of e-governance, government is expected to deliver its services to the citizens on 24*7 basis. To achieve this, the government has to set up a sound and stable infrastructure operational round the clock.

– Internet Data Centre is a facility which provides extremely reliable and secure infrastructure for running Internet operations on a 24*7 basis. It shall not at all be cost effective if each department starts setting up its own data centre as running a high class Internet Data Centre needs a lot of recurring resources.

– It is, therefore, suggested that the government may set up a high grade Data Centre at a National level to be used by all entities of the government.

– All departments should, in turn, establish high speed connectivity with the data center so that they can manage their applications from their own premises in a secured manner.

– In cases where the country is large and the government feels that one Internet Data Centre may not suffice, it could decide to set up multiple Data Centers.

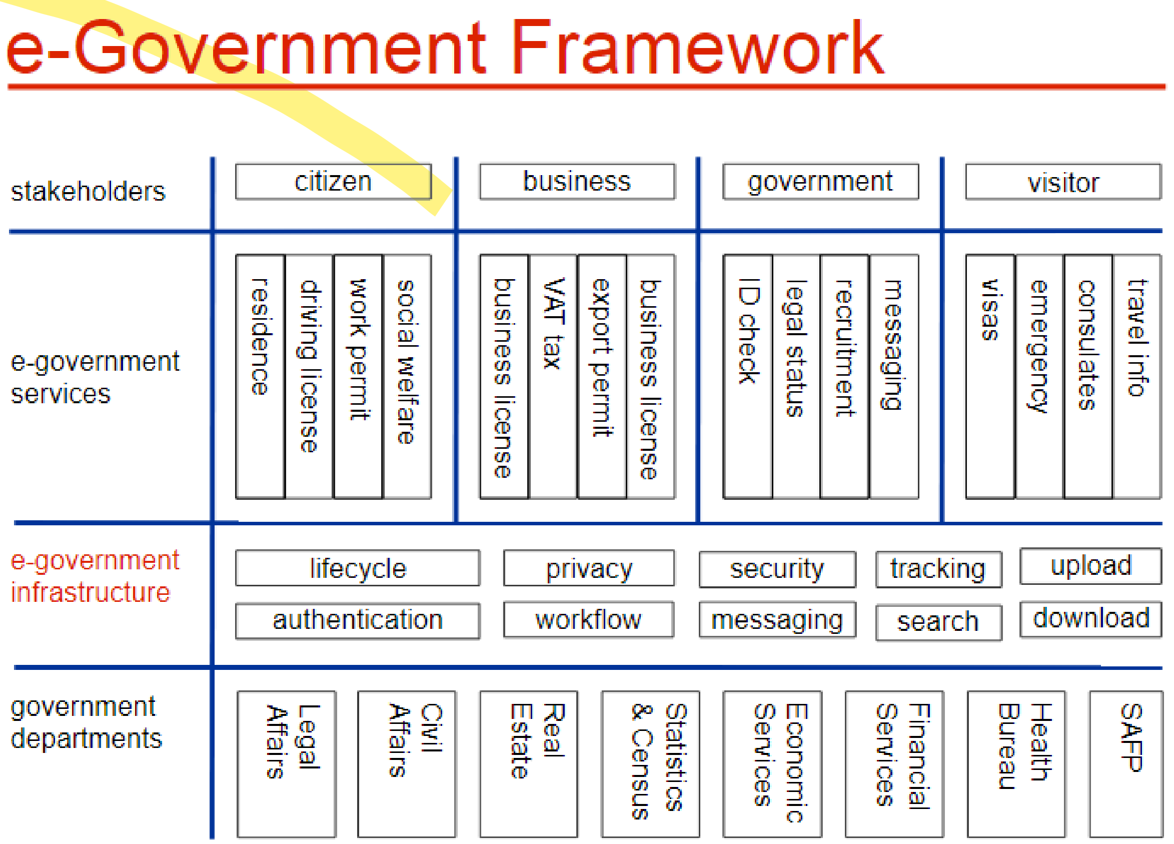
– However, the number of data centers should be optimized to the extent possible primarily due to the high recurring operative costs as well as scarcity of skilled resources.

- It is suggested that the decision to set up a data center should be driven by demand and not by political or geographical boundaries within the country.
- As the pace of e-government picks up nationwide, besides delivery of services, Government may also have to set up data centers to share the large scale/special purpose resources for development of the systems.

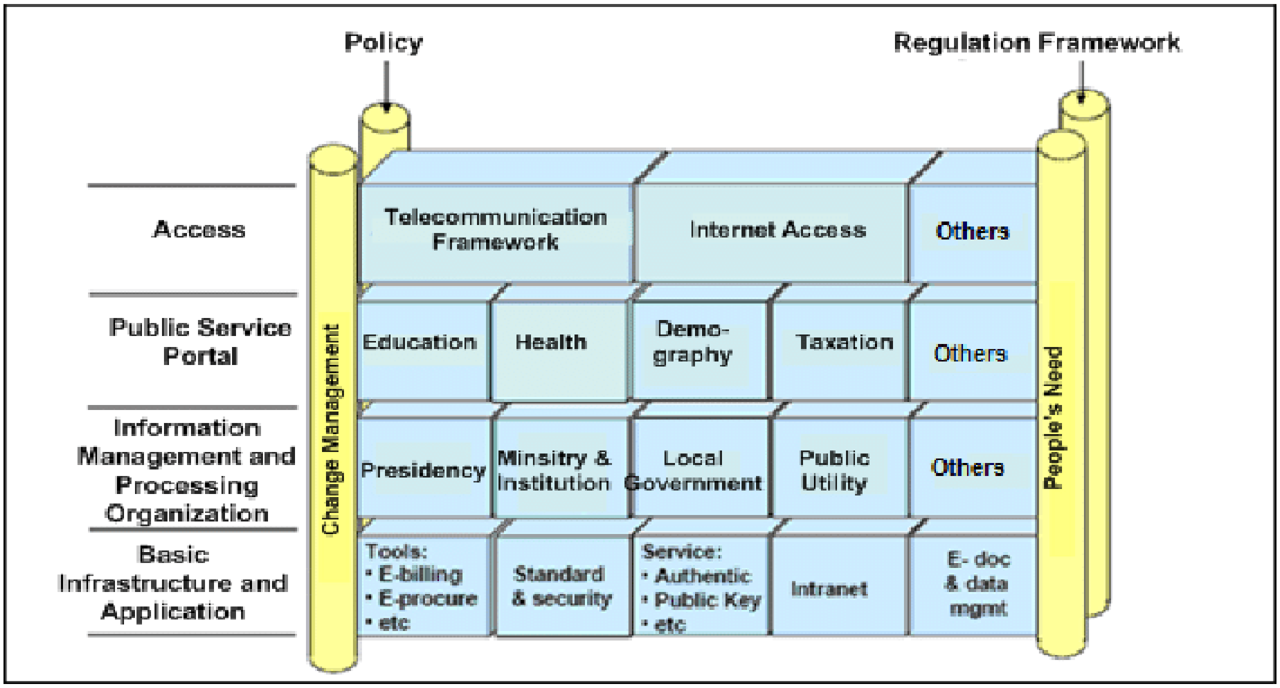
An Internet Data Centre should essentially have the following features:

- High End Computing Infrastructure
- Storage Networks (SAN/ NAS)
- High Speed Local Area Network
- Multi-Tier Security
- High Speed Internet Connectivity
- 24*7*365 Help Desk
- Multi-level Redundant power back-up
- Air Conditioning Management
- Fire Detection & Control System

E-government Architecture Framework:



Or



E-government Architecture generally consists of three components : Services Architecture, Process Architecture and Data Architecture

Services Architecture:

- Describes the whole lot of services offered by the Government, processes to be followed for each service, Concerned Department(s), relation/dependence on other services etc. Services could be like Vehicle Registration, Passport Issuance, Caste Certificate, Payment of Tax, etc.

Process Architecture:

- Lists the various processes to be followed for rendering different services, independent of their association with one or more services.
- These processes are then further grouped in various categories and detailed rules/procedures are defined for executing each of the processes.
- This brings a lot of standardization across services and promotes interoperability as well as reuse of process components.
- Processes could be Content Management, Citizen Registration, Personalization, Online Form Submission, Electronic Payment etc.

Data Architecture:

- Deals with the data associated with various Government Services, as described in service architecture.
- In Data Architecture, we enlist all the data elements needed/associated with above service and then define metadata about each data element.
- This metadata information includes the standard Nomenclature for each data elements, their type, size, format, default value, valid value range, owner etc.

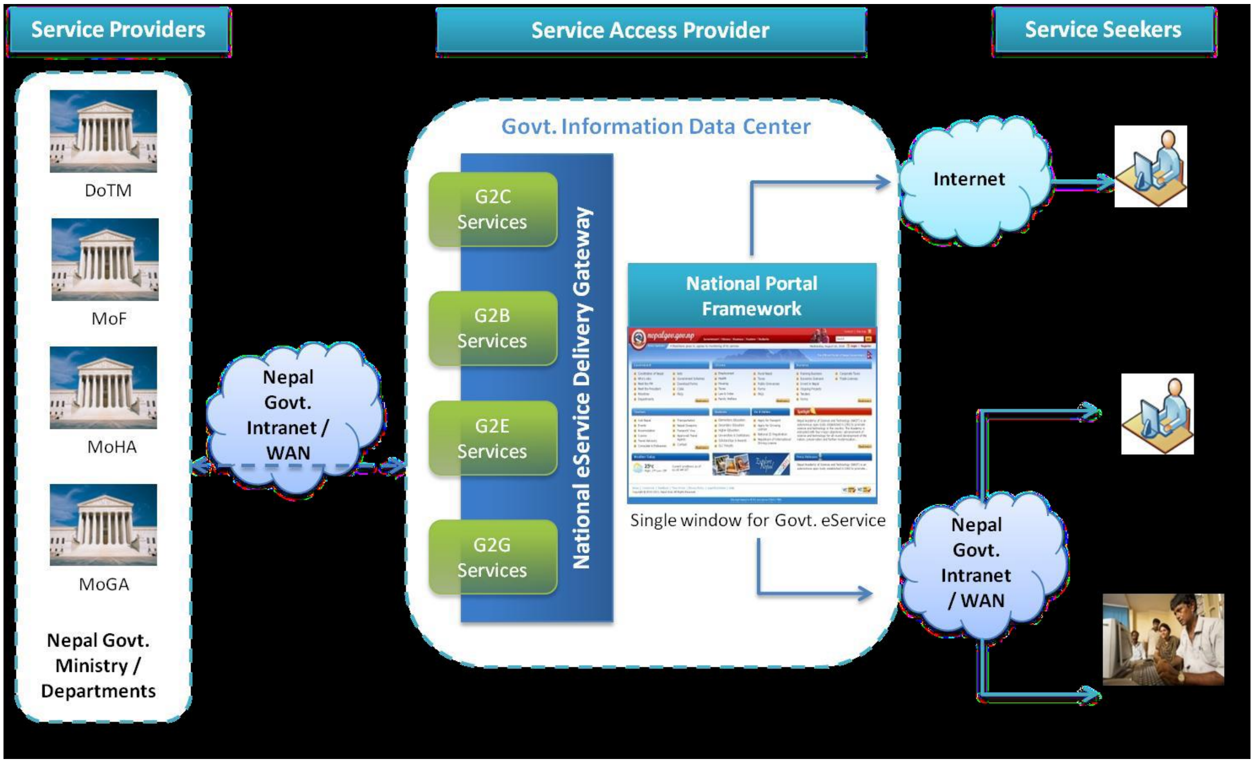
- Use of such a standard definition by all government applications shall facilitate interoperability among various applications as well their integration which shall go long way in delivery of integrated/ one stop services to the citizens and businesses.

E-Government Architecture of Nepal

All the eService's and electronic information in Nepal will be delivered via a comprehensive integration service delivery platform **—National e-Service Delivery Gateway||** which services as the gateway for electronic information exchange and interactions in Nepal. Government **eService Provider** typically back-end ministry / departments / government agencies will put up its service be it G2C, G2B, G2E or G2G for electronic delivery through the National eService Delivery Gateway. All the government and public e-Services (electronic Services) will be compliant with the GEA specifications.

The National eService Delivery Gateway & National Portal of Nepal will serve as the **Service Access Provider** that will provide the infrastructure to facilitate government service access by the Service Seekers. Linked to the Service Access Providers will be the delivery channels, which would be the access mechanism for the citizens and businesses to avail the e-governance services.

The Nepal **National Portal** will act as the single window one-stop store for the delivery of Govt. G2C, G2B & G2E eServices. **E-Service Seekers** typically citizens, business, government employee & tele-center users can avail these service by logging into the national portal and filling & submitting the service request forms online.


Service Providers
Service Access Provider
Service Seekers
DoTM
MoF
MoHA
MoGA
Nepal Govt. Ministry / Departments
Nepal Govt. Intranet / WAN
Govt. Information Data Center
G2C Services
G2B Services
G2E Services
G2G Services
National eService Delivery Gateway
National Portal Framework
Single window for Govt. eService
Internet
Nepal Govt. Intranet / WAN

Interoperability Framework:

Interoperability is defined as system ability to share and integrate information and work processes using a set of standards. One solution to the interoperability problem is using Grid technology. Open grid services aim for the integration of services across distributed and heterogeneous virtual organizations with disparate resources and relationships.

Data and information integration is important among government agencies. It needs to formulate methods and technology of collaboration. The requirements of a broader and comprehensive data interaction among government agencies, especially in the use of data and information together should be encouraged.

Interoperability concepts and strategies are crucial agenda of the national e-Government development to achieve integrated, safe and efficient utilization of data and information.

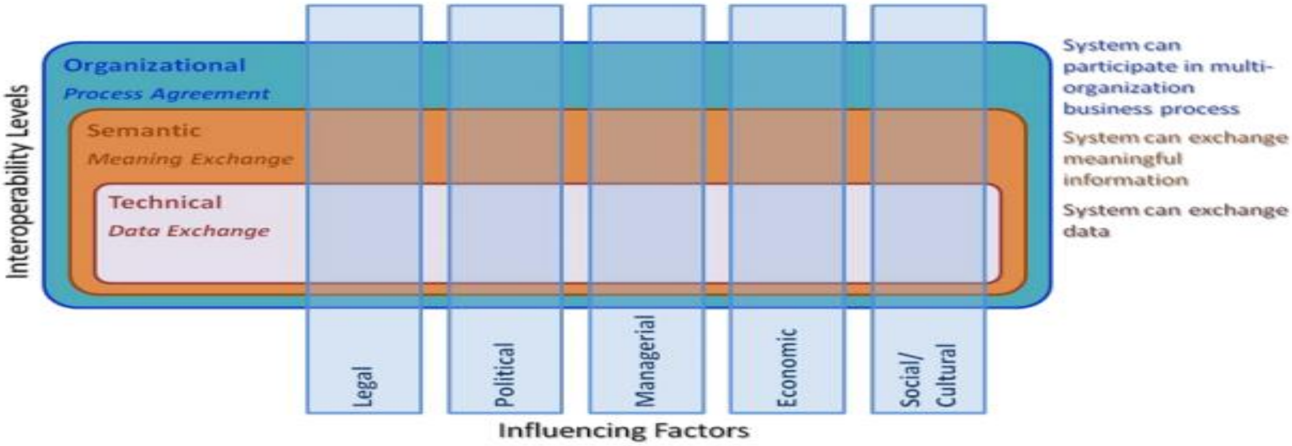
Interoperability in e-Governance is defined as "the ability of different systems from various stakeholders of e-Governance to work together, by communicating, interpreting and exchanging the information in a meaningful way". The interactions between all stake-holders are achieved, by sharing of information and knowledge through the business processes they support.

There are **three primary goals associated** with achieving interoperability in any system (computer or otherwise) i.e.

– **Data exchange** through Infrastructure and Software (Technical ability of software / hardware used by different systems to exchange data through common data exchange protocols, development of software necessary for management of data connections, creation of user interfaces in order to enable communication between different organizations).

– **Meaning exchange** (Ability of different systems / organization's to understand exchanged data in same way through a mechanism allowing the presentation of service data and data definitions).

– **Process agreement** (Ability of organization's to provide services to other organization's or their clients; It ensures services agreements and their legalization).



Government Integrated Data Center(GIDC):

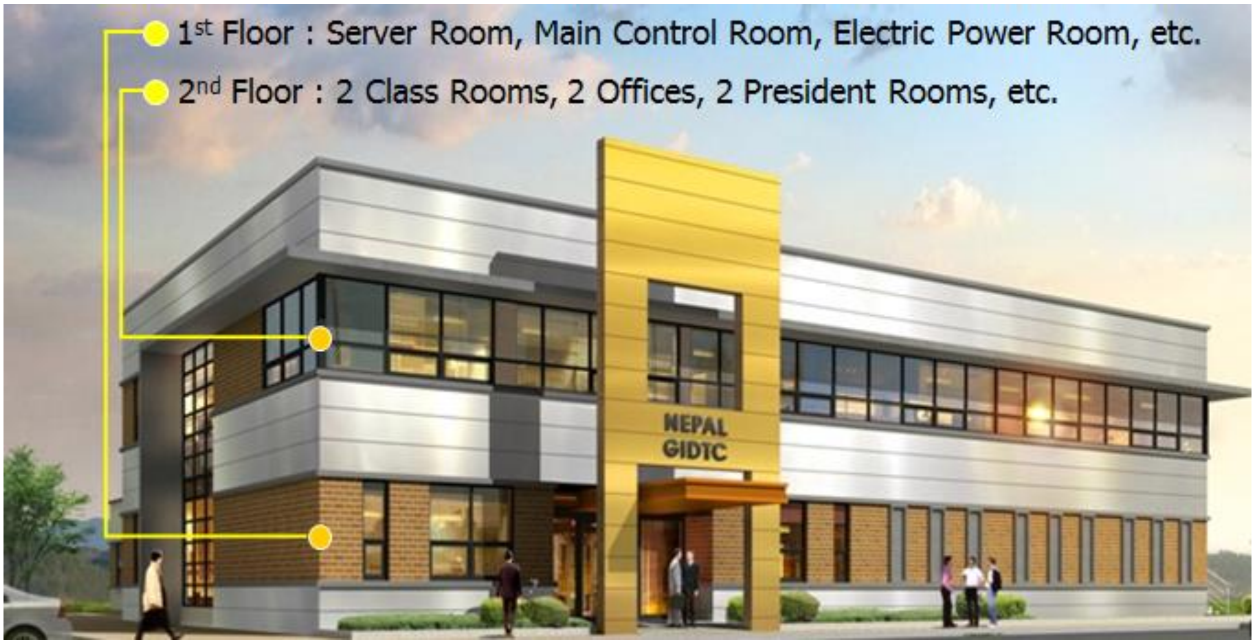
- The concept of GIDC was first envisioned in the national e-Government master plan (eGMP) developed by NITC[National Information Technology Center] and HLCIT[High Level Commission for Information Technology] with support from Korean IT Industry Promotion Agency (KIPA), which also defined the practical vision of national e-Government including various aspects like e-Government framework, architectures, infrastructure, organizational structure, implementation plan etc.
- Then Government of Nepal requested KOICA [Korea International Cooperation Agency] for the construction of GIDC and MOU [memorandum of understanding] was signed in September 19, 2007 between Government of Nepal and Republic of Korea for the construction of GIDC.
- The construction of GIDC was completed and handed over to NITC in March 11, 2009.
- Currently NITC is managing and operating the GIDC.

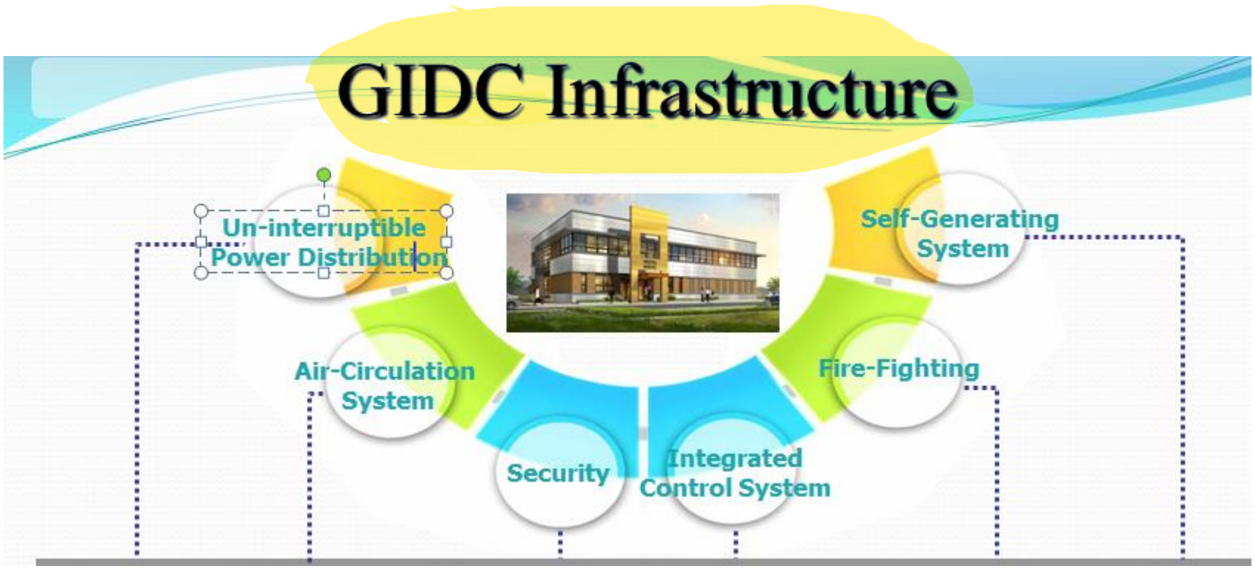
Objectives:

- Improve the IT infrastructure for e-Government by advancing GIDC in Kathmandu
- Provide the basis for Integrated Application Administration of e-Government Portal, e-Administration etc. through the construction of GIDC.
- Acquire ICT human resources and ICT competitiveness through the construction of ICT training facilities.
- Contribute to narrowing the digital divide and enhance the ICT cooperation between Nepal and Korea.

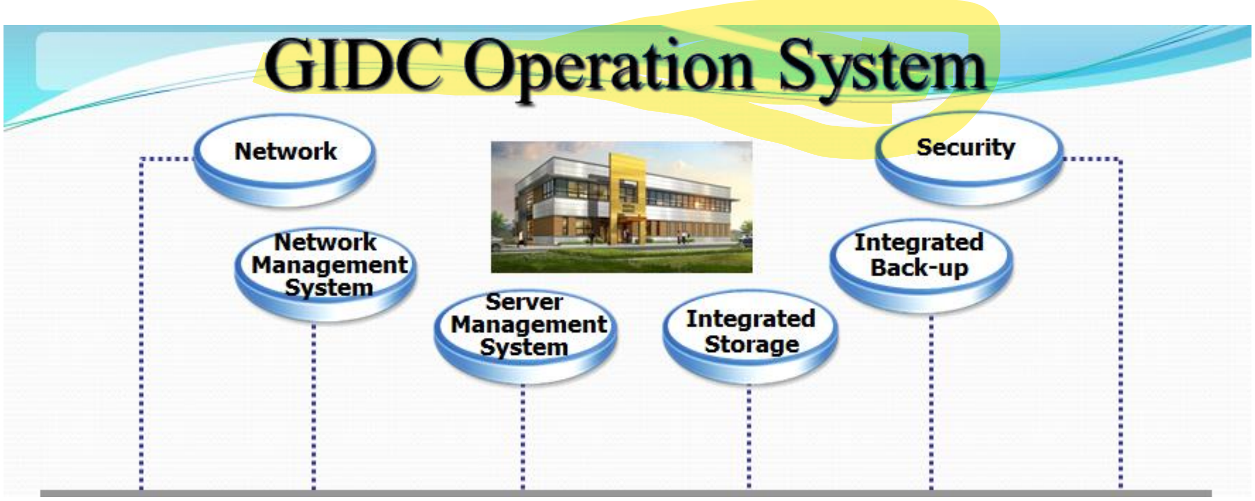
GIDC Construction:

- **Land Area : 2,034.76㎡**
- **Construction Area : 1,070.50 ㎡**
- **Aggregate Site Area : 1,601.50 ㎡**
- **Construction : 2 floors, 15 parking space**


1st Floor : Server Room, Main Control Room, Electric Power Room, etc.
2nd Floor : 2 Class Rooms, 2 Offices, 2 President Rooms, etc.
NEPAL GIDTC



- **Un-interruptible Power Distribution:**
  - Electricity Distribution System,
  - UPS Battery,
  - Emergency Lighting Grounding
- **Air-Circulation System**
  - Temperature & Humidity Control System , Air-Conditioning (and heating)
- **Security**
  - Trespassing Management System
  - CCTV
- **Integrated Control System**
  - Integrated Real Time Monitoring
  - FMS (Facility Management System)
- **Fire-Fighting**
  - FM-200
  - Self-Sensing System
- **Self-Generating System**
  - Digital Control Type Generator (380/220V 50Hz, 400KW)



- **Network:** Router Backbone Switch etc.
- **Network Management System:** Integrated Network Management System
- **Server Management System:** integrated Server Management System
- **Integrated Storage:** Integrated Storage, MSA 1500 16TB
- **Integrated Back-Up:** Integrated Back-up,10TB
- **Security:** Check Point Integrated UTM GW, Spam/Virus mail Prevention

Features of GIDC:

- High End Computing Infrastructure
- Storage Networks (SAN)
- High Speed Local Area Network
- Multi-Tier Security
- High Speed Internet Connectivity
- 24*7*365 Help Desk
- Multi level redundant power back-up
- Air Conditioning Management
- Fire Detection & Control System

4

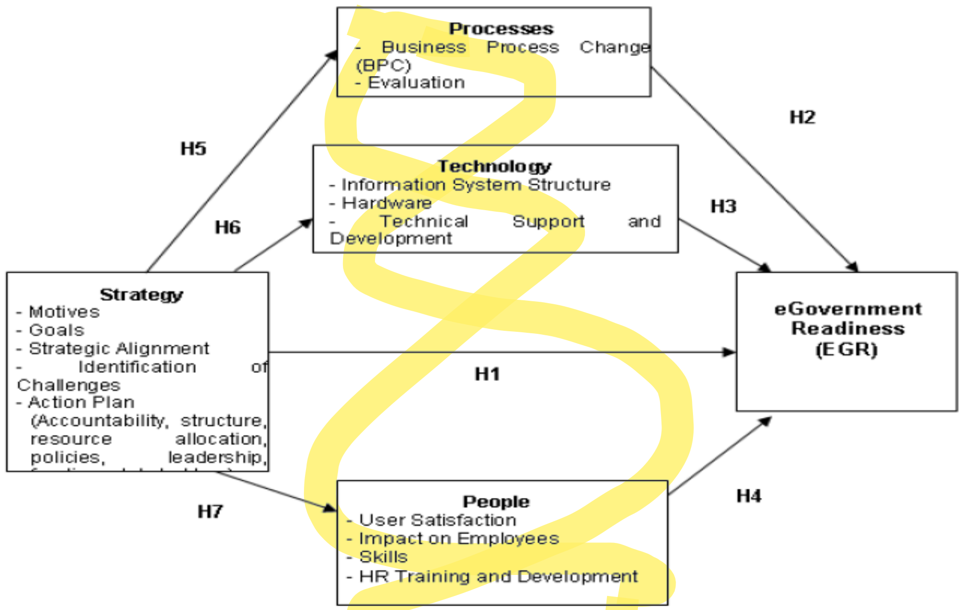
E-Readiness:

- The maturity of citizens, business, NGOs and governments for participating in the electronic world (i.e., e-commerce, e-governance, e-payment, etc.).
- e-readiness as the degree to which a community is prepared to participate in the Networked World - a world in which everyone, everywhere, has the potential to reap the benefits of connectivity to the network.
- E-readiness as the "state of play" of a country's ICT infrastructure and the ability of its consumers, businesses and governments to use ICT to their benefit.
- E-readiness as the degree to which an economy or community is prepared to participate in the digital economy.
- Country capacity and state of preparedness to participate in the electronic world.
- The state of maturity is commonly measured by the country's ICT infrastructure and the utilize the positive impacts of ICT for sustainable development.

E-readiness Infrastructure Prerequisites:

- Data system infrastructure
- Legal infrastructure
- Human infrastructure
- Institutional infrastructure
- Technological infrastructure
- Leadership and strategic planning

E-readiness framework:


Processes
- Business Process Change (BPC)
- Evaluation
Technology
- Information System Structure
- Hardware
- Technical Support and Development
Strategy
- Motives
- Goals
- Strategic Alignment
- Identification of Challenges
- Action Plan (Accountability, structure, resource allocation, policies, leadership,
People
- User Satisfaction
- Impact on Employees
- Skills
- HR Training and Development
eGovernment Readiness (EGR)
H1
H2
H3
H4
H5
H6
H7

The concept of e-readiness, though simple to understand in general terms, gets complex when we want to be analytical and to attach numbers to its components so as to compare different countries, states or agencies on their e-readiness. The framework, schematically represented in table, enables us to understand e-readiness in a degree of detail that permits meaningful surveys and measurements to be undertaken.

Indicators of e-Readiness		
Component of e-readiness	**Sub-Component**	**Indicators of e-readiness**
1. Policy	1.1 ICT Policy	Communication Policies
		Policy on ISP
		Incentives to ICT Industry
		Recognition of quality
		Facilitation of Growth & Promotion of Exports
	1.2 e-Government Policy	e-Government Vision
		Periodization of services
		PP Policy
		Policy on ESD (Electronic Service Delivery)
	1.3Architecture & Standards	Functional Architecture
		Technical Architecture
		Technical Standards
	1.4 Security Framework	Security Policy
		Privacy
	1.5Regulatory Framework	Cyber law
		IPR Protection
2. Infrastructure	2.1 Networks	National Backbone(s)
		Distribution Networks
		LANs & WANs
		Satellite & Wireless Networks
	2.2 Access	PC Penetration
		Internet Penetration
		Last Mile Connectivity
	2.3 ICT Hardware	Data Centre
		e-Government Gateway
		Payment Gateway
		Public Key Infrastructure
3. Resources	3.1 Political Resources	Leadership & Vision

		Continuity of Support to ICT sector
	3.2 Human Resources	IT Education & Training Institutions
		Expenditure on R & D in ICT
	3.3 Employee Resources	Champions of ICT
		Chief Information Offices,
		Access to PC & Internet Usage
4. Usage	4.1 Usage by Citizen	e-Mail & Internet Usage
		e-Literacy
	4.2 Usage by Businesses	e-Commerce
		e-CRM, e-SCM
		e-Procurement in B2B & G2B Areas
	4.3 Usage by Government	No. of Web Sites/Portals
		No. of e-Services; e-Transactions
		No. of e-Government Projects
		Extent of G2G usage

The e-readiness framework consists of assessing readiness along four fronts- policy, infrastructure, resources and usage. Each of the four components consists of 3-5 sub-components that enable a deeper understanding of the state of each of the major components. A set of 43 indicators is suggested as a drilldown of the sub-components to enable quantitative and qualitative assessment of e-readiness.

Steps to e-Government readiness

The exhibit shows the 10 step process to e-government readiness that can act as guide for improving the score of e-government readiness. It is not necessary to follow the 10 steps sequentially. Some of them can be implemented in parallel. Each step may be broken down into a set of tasks and pursued for effective results. In fact, some of the steps and components, such as design of architectures, the CIO program, setting up of a state data centre and gateway, are themselves very large initiatives.

Ten Steps to e-Government Readiness

1. Articulate the e-government vision and strategy. Prepare a five-year perspective plan.
2. Review the Telecommunications policy, to promote an open, competitive environment for creation of national and sub-national networks.
3. Prepare a list of G2C and G2B services that citizens and businesses need to be provided electronically.
   Prioritize the services.
   Announce a policy on Electronic Service Delivery.

4. Design Functional and Technology Architectures that are aimed at delivering the e-services.

   Prescribe standards for security.
5. Initiate statewide e-government projects adopting the pilot approach. Ensure these are part of the 'big picture' developed in Step 4.
6. Design and implement an appropriate CIO program.

   Implement change management programs across all major government agencies.
7. Ensure that all government agencies earmark 2-5% of their budgets to e-government.

   Announce a PPP policy for e-government and take up a few projects adopting the PP model.
8. Establish a government-wide WAN for data, voice and video for G2G applications, adopting a PPP model.
9. Enact a cyber law that gives a legal validity to all electronic transactions and records and permits use of digital signature for authenticating messages and documents.

   Public policies on security and privacy for e-government
10. Establish data centers for e-government using the PPP model. Design and establish an e-government gateway at the State Data Centre.

Issues in e-Government Readiness

Getting a country into a stage of e-readiness requires a multipronged effort. While it is possible to adopt a structured approach, it is fraught with several problems. It is necessary to look at three issues which are cross-cutting in nature- people readiness, reform readiness, and the readiness for sustainability.

Issue 1: People readiness

We can program processes. We cannot program people. There lies the problem - in getting people ready for e-government. People readiness has four stages of evolution.

1. Readiness to think
2. Readiness to lean
3. Readiness to act
4. Readiness to transform

i. **Readiness to think** of e-government is to do with the change of mindset and is by far the most difficult one to achieve. It is overcoming the internal resistance to the flow of new ideas.

   Getting people **ready to think** of e-government involves conducting a series of workshops involving 'external' experts who have the first-hand experience in having implemented e-government successfully. This stage also requires a continuous 'evangelizing' (convert or seek to convert).

ii. **Readiness to act** is a hands-on-exercise. It is believed that giving a person a PC and exposing to the Net is a good way to initiate him or her into the e-world and getting people hooked on to 'Act'.

iii. **Readiness to transform** is the final stage where people in the organization start acting as teams, willing to spare an extra hour to improvise, improve, innovate and transform the workplace and service centre.

Issue 2: Reform readiness

E-government efforts end up as 'old wine in new bottle' unless these are accompanied by an urge to transform the way government functions and treats it customers. This is possible through an extensive exercise to reform the processes and the legal provisions underlying them. Reform is triggered by the need to introduce new services and to provide the existing services in a new way to the citizens, in a manner that is convenient and cost effective from the citizen's viewpoint.

Transforming the government involves redefining services cutting across the boundaries of delivery channel, agencies, departments and ministries. This in turn involves reforming processes, forms, procedures, Rules and Acts.

Introduction of single window service of registration demands, merging of forms, rewriting of procedures, passing of new rules and an integrated legislation that cuts across the agency jurisdictions.

Reform readiness, therefore, means readiness of the political and legislative bodies to change the laws of the land and readiness of the administrative functionaries to think laterally and create new processes and new services.

Issue 3: Backend readiness vs. Front end readiness

One of the classic conflicts that arise in the course of a serious implementation of e-government is the one between the 'backend readiness' and 'front-end-readiness'.

By 'backend readiness' we mean the following tasks:

Developing backend systems

- Design of e-services
- Business process reform
- Development of application software
- Pilot and rollout

Establishment of infrastructure

- Establishment of a data centre
- Setting up of hardware at all agency locations
- Networking of all backend systems

Readying the people

- Creation of a cadre of CIOs
- Training
- Change Management

Front-end readiness means the following:

- Creation of a delivering channel policy
- Establishing service centers /kiosks
- Creation of Websites and portals

Emphasis on the front-end readiness would produce quick results and impact in the short run. This is definitely necessary in generating the excitement required to attract people-employees and citizens-to what e-government can do. Launching of information websites, online statistical systems etc. are typical examples of the eagerness to bring in quick visibility through front-end cosmetics. However, excessive stress on the front-end without backend readiness is dangerous.

Security for e-Government:

Security is all about protecting the Information and Communication Technology (ICT) assets of an organization.

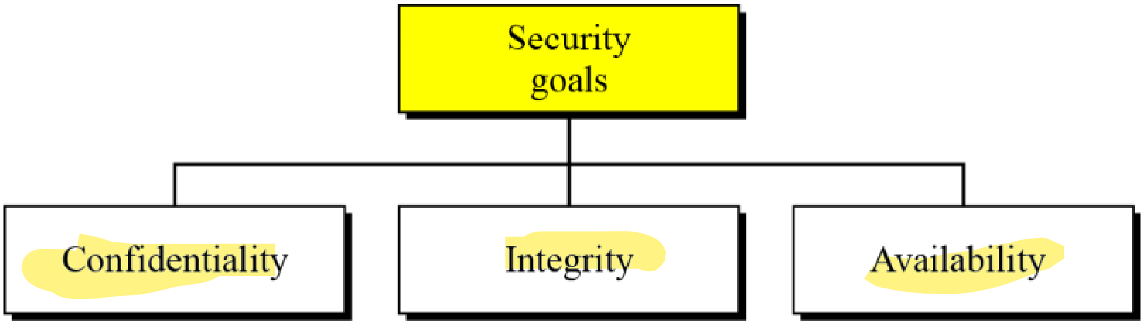
E-Governance involves Information Technology enabled initiatives that are used for improving the interaction between Government and citizens or Government and business as well as the internal Government operations. To provide “trusted” services, e-Governance needs to focus on Effectiveness, Efficiency, and Flexibility & Transparency.

If the citizen or end user is to derive maximum benefit from the provision of e-Services through e- Governance, the e-Service must possess the following attributes.

- The users must know the information about the available e-services;
- The users must be aware of the benefits of these services;
- The user should be able to locate the e-services easily;
- The e-services must be accessible to all members of the intended target groups;
- The information from the e-services should be comprehensive, correct, readily available, and easy to understand with respect to language and structure;
- The provision of e-services should be confidential, and in no way violate the privacy of either party;
- The design of e-Governance applications should comply with the existing legal data protection requirements and relevant legal and statutory laws & acts.

From the attributes it becomes evident that the “value” of information held and processed by the e-Governance service needs to be protected at all levels (i.e. Application, Infrastructure, and Operation & Management). Information security is intended to safeguard the information assets and is determined in terms of confidentiality, integrity and availability.

Security goals



- **Confidentiality**: Confidentiality, keeping information secret from unauthorized access, is probably the most common aspect of information security: we need to protect confidential information. An organization needs to guard against those malicious actions that endanger the confidentiality of its information.

- **Integrity**: Information needs to be changed constantly. In a bank, when a customer deposits or withdraws money, the balance of their account needs to be changed. Integrity means that changes should be done only by authorized users and through authorized mechanisms.
- **Availability**: The third component of information security is availability. The information created and stored by an organization needs to be available to authorized users and applications. Information is useless if it is not available. Information needs to be changed constantly, which means that it must be accessible to those authorized to access it. Unavailability of information is just as harmful to an organization as a lack of confidentiality or integrity. Imagine what would happen to a bank if the customers could not access their accounts for transactions.

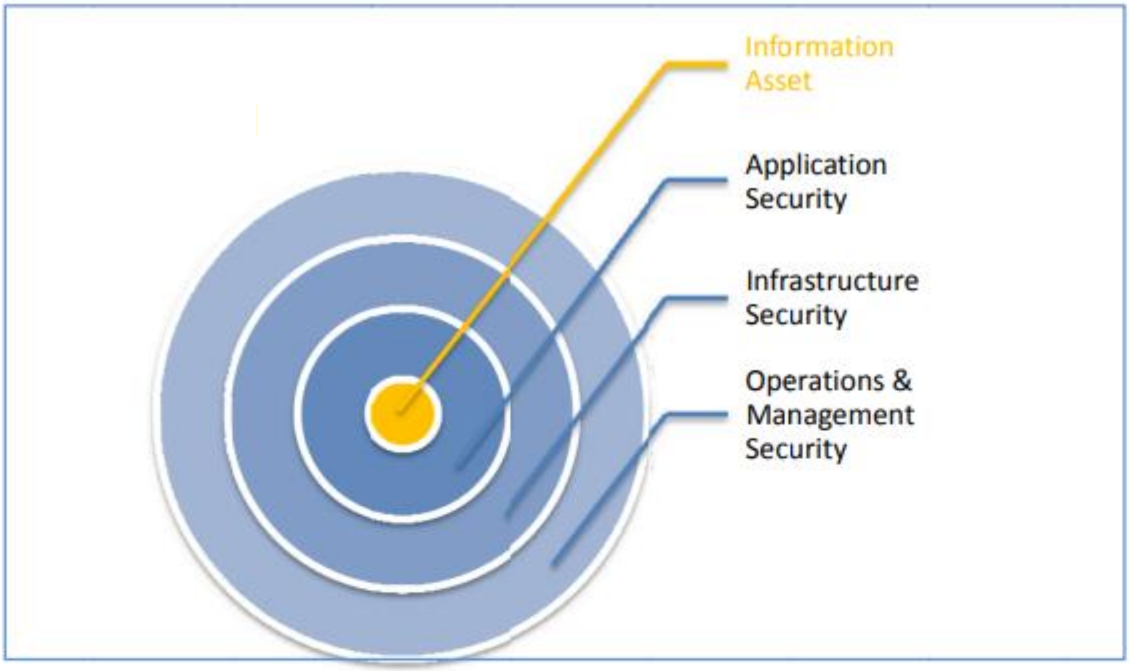


Figure 1: Security Layers

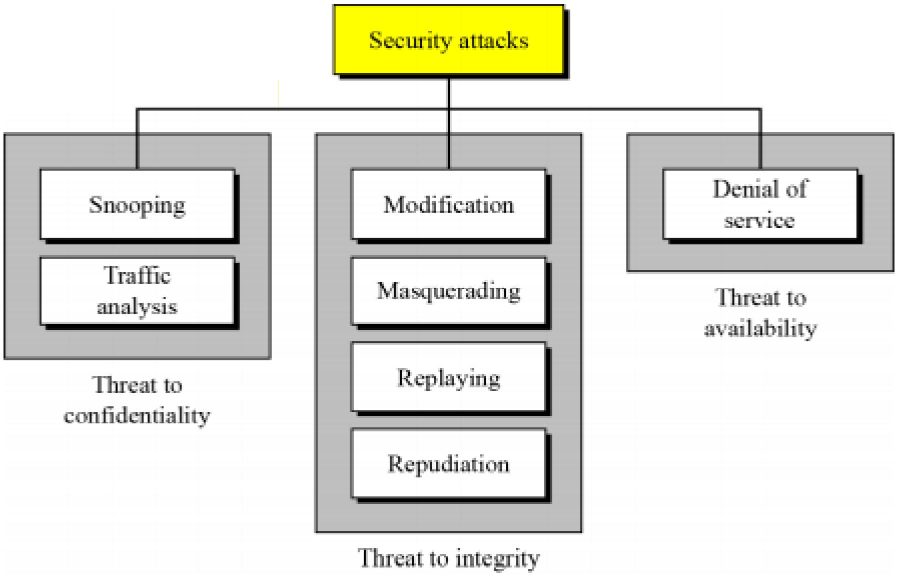
E-governance security which is based on specially two terms i.e. "**Security of What**?" and other is "**Security against what**?"

The ICT assets themselves can be of a wide variety including the following: **Data, Information, Knowledge Resources, Programs, Hardware, Networks**, above we mention some ICT assets which are very important for security perspective of E-governance. This is a very important responsibility of E-governance administrators to protect these assets.

Sources of threats and then some types of threats which affect to E-governance:

Sources of Threat: The sources of threat can be **internal** or it can be **external** to the government body. There are various internal sources of threat like the **employees** who work on the E-governance project, **customers** of the E-governance projects they may attempt to access the databases for their personal financial profit. When we talk about external sources it may be **Professional hackers, Criminal organizations, various Intelligence agencies or Investigation agencies.**

Types of Threat:



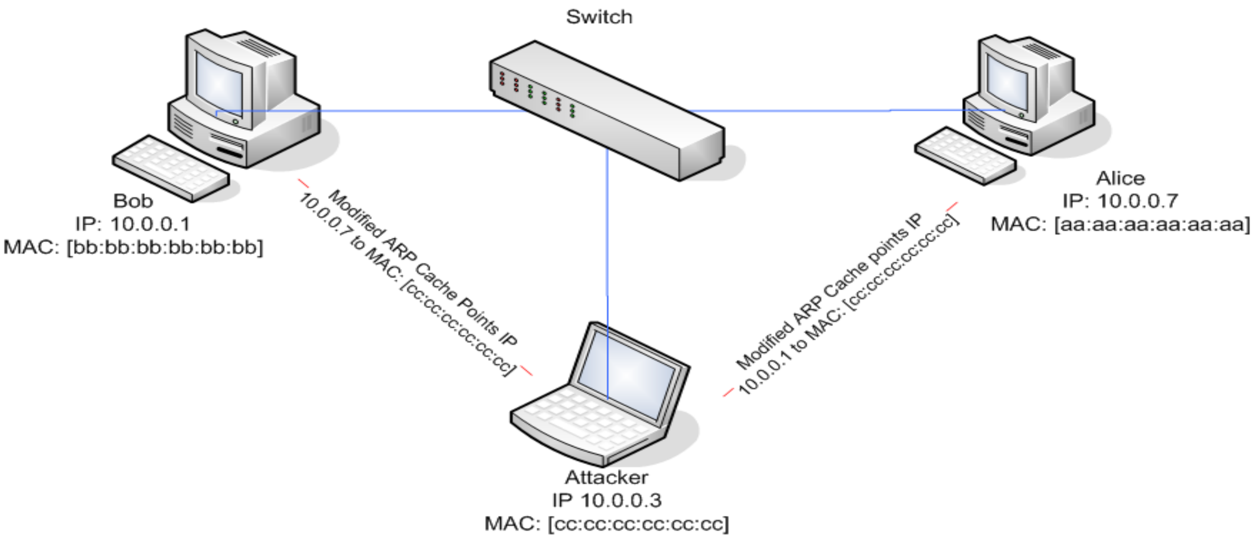
Threats may include unauthorized access, modification, and destruction of data. The threats may be of different types varying from time to time because technology changes frequently. The attacks on security of e-governance system can be in different forms including- Defacing of web sites, Hacking, Cracking, Damage to critical database and applications, Network security check list, Viruses and Malwares etc. the damage of ICT assets need not always be a result of such malicious attacks as mentioned previously. It may be some kind of natural or environmental disasters etc.

1. **Sniffing**

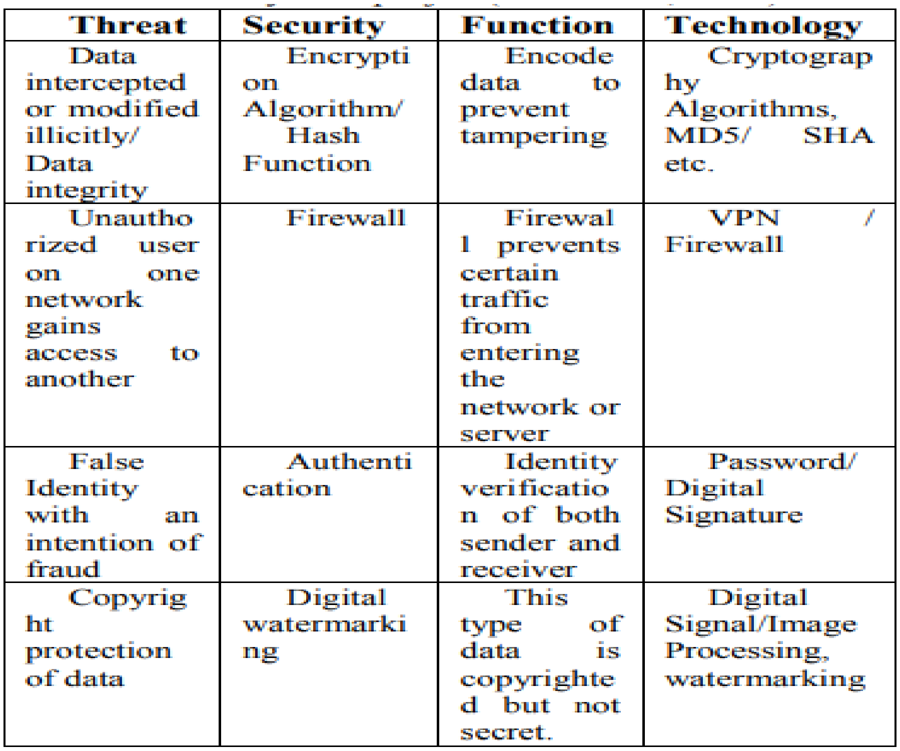
   Sniffing is the process of monitoring and capturing all the packets passing through a given network using sniffing tools. It is a form of “tapping phone wires” and get to know about the conversation. It is also called **wiretapping** applied to the computer networks.

2. **Spoofing**

   Spoofing is the act of disguising a communication from an unknown source as being from a known, trusted source.


Switch
Bob
IP: 10.0.0.1
MAC: [bb:bb:bb:bb:bb:bb]
Alice
IP: 10.0.0.7
MAC: [aa:aa:aa:aa:aa:aa]
Modified ARP Cache Points IP 10.0.0.7 to MAC: [cc:cc:cc:cc:cc:cc]
Modified ARP Cache points IP 10.0.0.1 to MAC: [cc:cc:cc:cc:cc:cc]
Attacker
IP 10.0.0.3
MAC: [cc:cc:cc:cc:cc:cc]

3. **Denial-of-service (Dos):** attacker sends large number of connection or information requests to a target § Target system cannot handle successfully along with other, legitimate service requests § May result in system crash or inability to perform ordinary functions
4. **Modification:** Some portion of a legitimate message is altered or that message are delayed or recorded to produce an unauthorized effect.
5. **Replaying:** Attacker obtains a copy of message sent by a user and later tries to replay it.
6. **Repudiation:** Senders of the message might later deny that she/he has sent the message; the receiver of the message might later deny that he /she has received the message.



Threat	Security	Function	Technology
Data intercepted or modified illicitly/ Data integrity	Encryption Algorithm/ Hash Function	Encode data to prevent tampering	Cryptography Algorithms, MD5/ SHA etc.
Unauthorized user on one network gains access to another	Firewall	Firewall prevents certain traffic from entering the network or server	VPN / Firewall
False Identity with an intention of fraud	Authentication	Identity verification of both sender and receiver	Password/ Digital Signature
Copyright protection of data	Digital watermarking	This type of data is copyrighted but not secret.	Digital Signal/Image Processing, watermarking

Security Issues in E-government:

In the designing of an efficient e-Government system, security becomes the main issues to be considered. E-Government system is type of on-line system that require a ICT based network to execute properly but e-Government system is different from other on-line system particularly with reference to security as an e-Government system handles a lot of secure and legal information that must be protected from unauthorized users. Some of the security issues in e-Government are discussed below:

- **Confidentiality**/Privacy/Accessibility: ensuring that systems and information are accessible to those authorized to access it
- **Integrity**: ensuring systems and data have not been tampered with (either accidentally or maliciously) and are in their original and intended state.
- **Accountability**/Non-repudiation: ensuring that when data is delivered to a recipient neither recipient nor sender can deny having received or sent the data.
- **Authentication**: ensuring that entities (whether individuals, hardware or software) can be authenticated as being the original and genuine entity.
- **Trust**: that there is an infrastructure both technical and non-technical which engenders trust and that this is made visible to the community of users.

1. Challenges – Security:

- **Data & Application security**
  - PPP models (service delivery model)
  - Lack of internal Technical capacities
    - Loopholes in the applications and databases
    - Knowledge transfer
    - Exit management
- **Complex e-Governance Projects**
  - High performance & response time
  - High Security desired on operations but not a top priority to start with
- **Multiple Legacy Environments**
  - security framework
- **Implementation of Security Standards**
- **Implementation of suitable access controls and authorization**
- **Preparation of RFPs[**Request for proposal**] which captures all the security requirements**

2. Security Management:

The security of the e-governance system has to be managed systematically in three levels; this model is explained with the help of this figure:

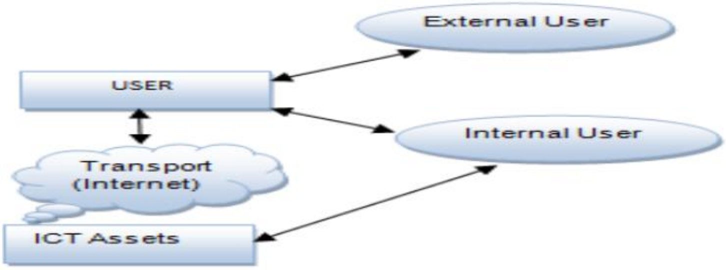
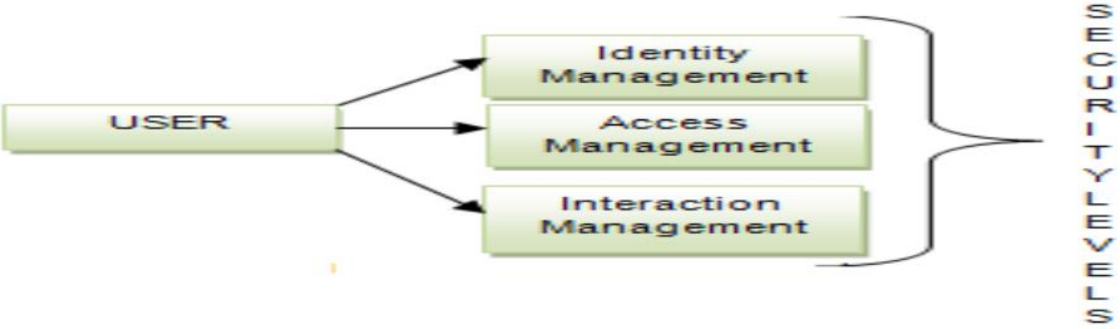


Fig: E-governance Security Environment

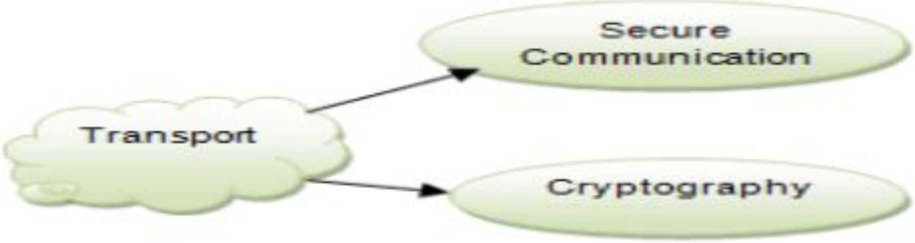
1. **Security at User Level Security** at user level is a very important issue. We can classify user level security management in three Parts:



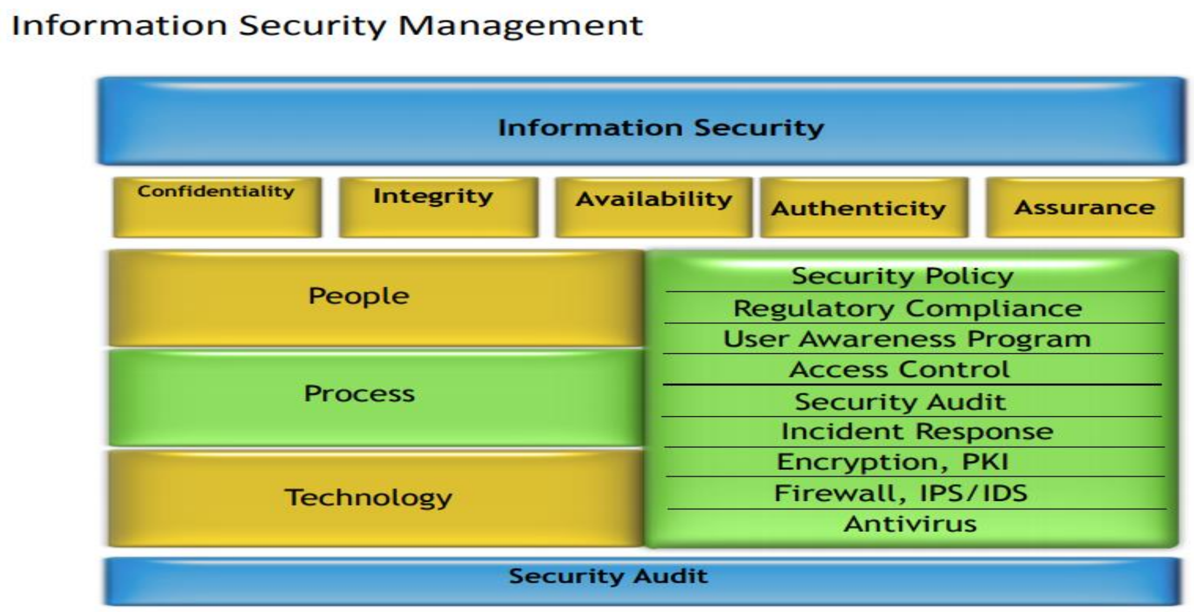
   - **Identity Management:** The main purpose of this is to create unique digital identity or credential to all legal users by providing a unique user name and **password**, to create and manage ICT systems which ensure that the digital identities are secure.
   - **Access Management System:** In this level the unique credentials which are provided to the user at identity level are matched to identify the user, that he/she is actually the authentic person
   - **Interaction Management System:** interaction management is a most comprehensive and complex phase. It includes assurance of the Integrity, Confidentiality and Non-repudiation principles of a comprehensive security. In user level, we can use various tools such as digital identity token, public key infrastructure (PKI), **digital signature**, asymmetric key **cryptography** etc. to provide or enhance the security at the user level.

2. **Security at Transport Level** In this level we consider about e-governance security in two aspects which are security within LAN and WAN, and the second one is Security over the Internet. This security level is classified into two systems, i.e. Secure Communication System and Cryptographic System.

   The data and information reaches through user to ICT assets or vice-versa, and when the data is in between these two i.e. in transmission medium which can be either LAN, WAN, or any wireless or any other medium whatever, then we need a higher security. For this e-governance administrator use various tools or techniques like creating a **Virtual Private Network** (VPN), installing **Firewalls**, using higher and complex **Encryption** or **decryption techniques** etc.



3. **Security at ICT Assets level ICT assets** are the most precious for any organization or institution, so to secure this level we have two broad categories of security treatment
   - **Physical Security** It is used to protect the data against physical damages or losses like- natural disasters etc. to protect data in this security level we take some steps such as- security level of data centers are highly secured by using biometric-controlled system, in data centers provision of dust-proof environment, fire protection systems, security alarms, CCTV monitoring of data center etc. automated backup system. By using some basic instructions we easily secure the data physically.
   - **Electronic Security** to give the protection against digital threats we want to use electronic security. We have various electronic security tools, and we can manage them in two categories:
     - **Anti-virus System** When we discuss about digital threats the first thing in our mind is virus, which affects our ICT assets in various ways such as- slowing down of the system, occupy disk space, corrupt our valuable data or storage medium etc. it is also known as malware, worms and Trojan horses.
     - **Firewalls**: A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.



4. E-governance Security Architecture:

The security architecture of E-governance is a high level document that set the security goals of e-governance project and describe the procedure that need to be followed by all the e-governance hierarchy such as users, businesses, operators etc. Appropriate legal framework is absolutely essential for the systematic and sustained growth of e-governance.

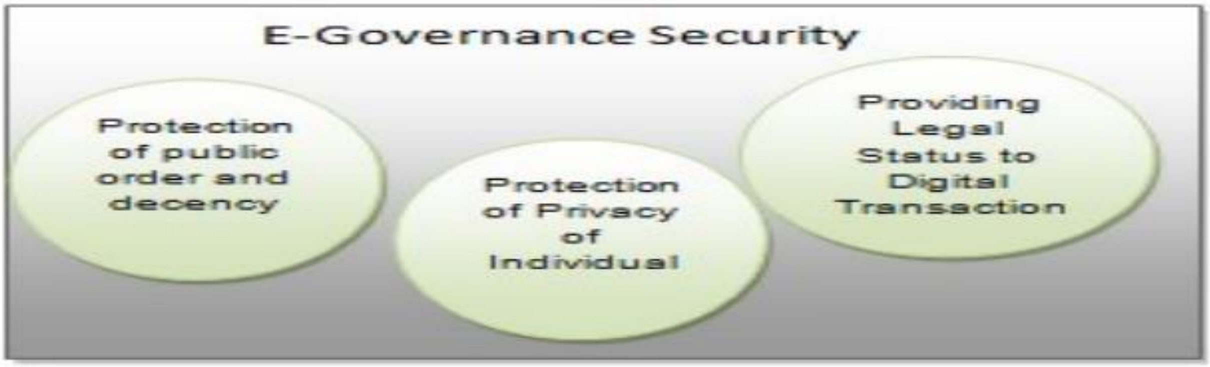

E-Governance Security
Protection of public order and decency
Protection of Privacy of Individual
Providing Legal Status to Digital Transaction

Fig.9- E-governance Security Architecture

Protection of Public Order and Decency:

The internet is a highly capable of being saturated and versatile medium at the same time. Its reach is very vast and due to its multimedia capability its impact can be immediate and profound. So the government has to beware of its potential to create a negative impact on society through promotion of terrorism, pornography, communalism, violence etc.

Protection of Privacy of Individuals:

Disclosure of personal information over the internet raises questions related to the privacy of individuals.

Providing Legal Status to Digital Identities and Transactions:

One of the fundamental requirements of e-governance projects is its ability to create and sustain the operations of government agencies as well as private agencies. So it's very necessary to consult legal status of entities and actions such as- 'legal status is to be provided to the digital identities', 'provide the legal recognition to digital assets', ' provide a digital authority to digital transactions, these transactions could be in the areas of G2G, G2B,G2C etc.'. 'Agreements and contracts in digital form'.

5. Security Standards:

- The standard for information security was set by the BS 7799, being its popularity it was adopted by ISO as ISO 17799 and its sequel BS 7799-2 that prescribes the specification for Information Security Management.
- "The ISO 27001 standard was published in October 2005, essentially replacing the old BS 7799-2 standard. It is the specification for an Information Security Management System.
- "ISO 17799 defines 127 security controls structured under 10 major headings to enable the information security manager to identify the particular safeguards that are appropriate to there specific area of responsibility.
    - **Security policy**
    - **Access control**
    - **Systems development and maintenance**
    - **Organization of assets and resources**
    - **Physical and Environmental security**
    - **Personnel security**
    - **Compliance**
    - **Communication and operation management**
    - **Asset classification and control**
    - **Business continuity management**

- **Security Policy** – provided management direction and support for information security.
- **Personal Security** – reduces the risks of human error, theft, fraud or misuse of facilities.
- **Access Control** – secures management of access to information
- **Compliance** – avoids breaches of any criminal and civil law, statutory, regulatory or contractual obligations and any security requirement.

- **Systems development and maintenance** – ensures that security is built into information systems at the design and development stage.
- **Communications and operations management** –ensures the correct and secure operation of information communication and processing facilities.
- **Organization of assets and resources** – helps to manage information security within the organization.
- **Asset classification and Control** – helps to identify assets and protect them appropriately.
- **Physical and environment security** – prevents unauthorized access, damage and interference to business premises and information.
- **Business continuity management** – avoids interruptions to business activities and protects critical business processes from the effects of major failures or disasters.

Protecting Internet Communications: Encryption

- **Encryption**: The process of transforming plain text or data into cipher text that cannot be read by anyone other than the sender and receiver
- **Purpose**: Secure stored information and information transmission
- **Provides**:
  - Message integrity
  - Nonrepudiation
  - Authentication
  - Confidentiality
- **Plain text**: the original message in human-readable form.
- **Cipher text**: the encrypted message
- **Encryption algorithm**: the mathematical formula used to encrypt the plain text.
- **Key**: the secret key used to encrypt and decrypt a message.

Encryption Algorithms

- **Private key encryption**
  - symmetric cryptography
- **Public key encryption**
  - asymmetric cryptography
- **Digital signature**

1. Private Key (secret Key) Encryption/Symmetric Key Encryption

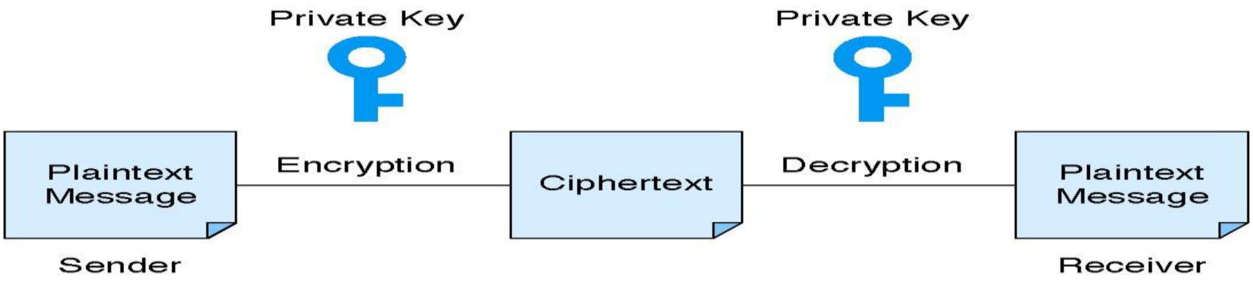
- The same key is used by a sender (for encryption) and a receiver (for decryption)
- The key must be transmitted to the receiver.

  Example:

  DES (Data Encryption Standard) algorithm with 56-bit key

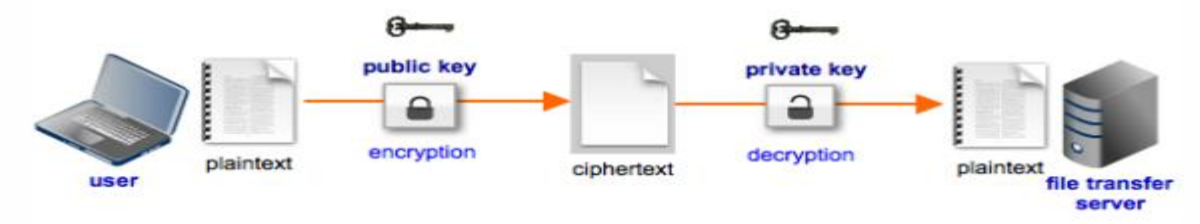
Data Encryption Standard (DES)

The standard symmetric encryption algorithm supported the NIST and used by U.S. government agencies until October 2, 2000.



2. **Public Key Encryption/Asymmetric Key Encryption**

- Uses two different keys: a public and a private key.
- Receiver's public key must be delivered in advance.
- Sender uses receiver's public key to encrypt the message and receiver uses private key to decrypt the message (Sender can be sure the receiver is the true receiver)
- Example:
  - RSA (Rivets, Shamir, and Adelman) algorithm with 512-bit to 1024-bit key.



So,

Public key encryption

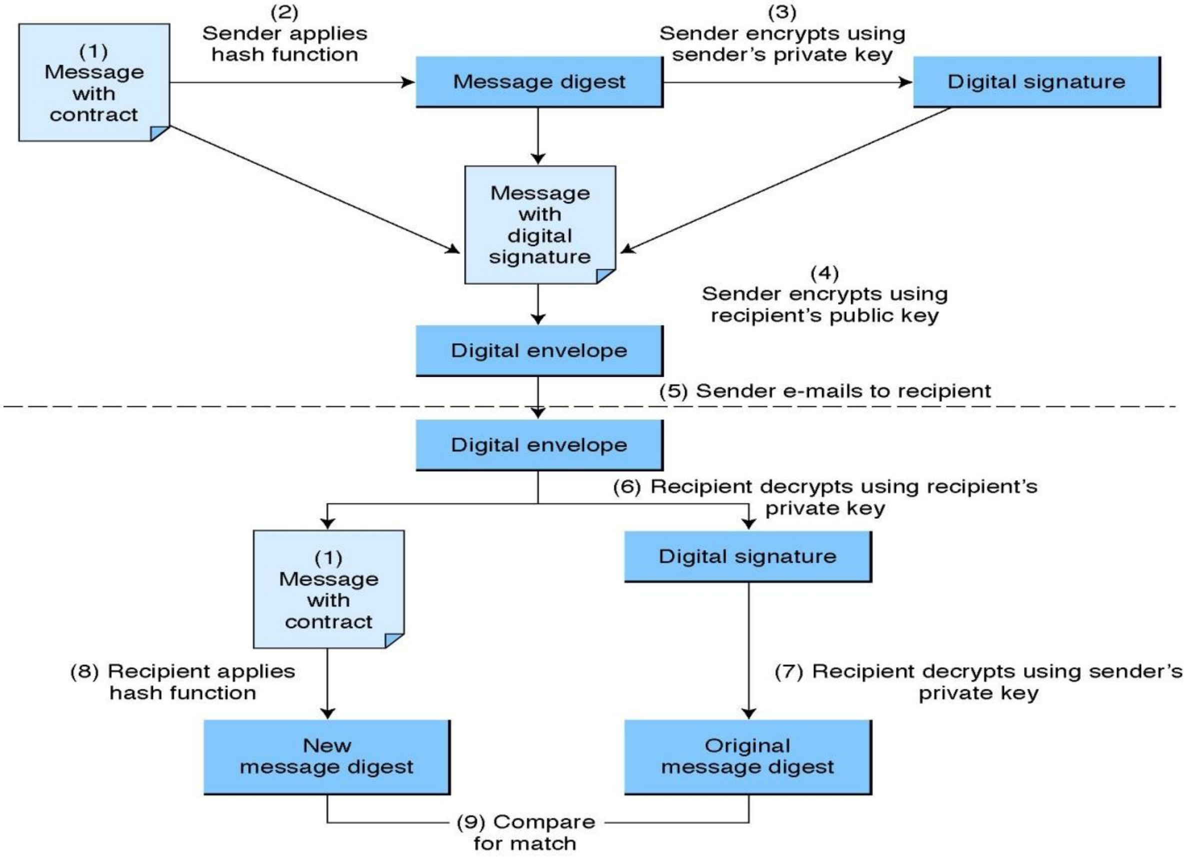
Method of encryption that uses a pair of matched keys—a public key to encrypt a message and a private key to decrypt it, or vice versa

Public key-Encryption code that is publicly available to anyone

Digital Signature

An identifying code that can be used to authenticate the identity of the sender of a document hash. A mathematical computation that is applied to a message, using a private key, to encrypt the message.

- It is used for the authentication and nonrepudiation of senders by applying public key encryption in reverse, and ensures the integrity of the message.
- How digital signature works:
  - Sender:
    - Create message digest: Hash(original message)
    - Digital signature: Encrypt(Message digest, Sender's private key)
    - Encrypted message: Encrypt(Original message, Receiver's public key)
    - Send the hash function, digital signature, and the encrypted message to receiver.
  - Receiver:
    - Use receiver's private key to decrypt the encrypted message to reveal the original message.
    - Use the sender's public key to decrypt digital signature and reveal the message digest.
    - Apply the hash function to the original message. If the hash value matches the message digest in the digital signature, the message is intact.


(1) Message with contract
(2) Sender applies hash function
Message digest
(3) Sender encrypts using sender's private key
Digital signature
Message with digital signature
(4) Sender encrypts using recipient's public key
Digital envelope
(5) Sender e-mails to recipient
Digital envelope
(6) Recipient decrypts using recipient's private key
(1) Message with contract
Digital signature
(8) Recipient applies hash function
(7) Recipient decrypts using sender's private key
New message digest
Original message digest
(9) Compare for match

Digital Certificates

- A digital certificate is a program embedded in a Web page that verifies that the sender or Web site is who or what it claims to be
- A certificate is signed code or messages that provide proof that the holder is the person identified by the certificate
- Certification authority (CA) issues digital certificates

Main elements:

- Certificate owner’s identifying information
- Certificate owner’s public key
- Dates between which the certificate is valid
- Serial number of the certificate
- Name of the certificate issuer
- Digital signature of the certificate issuer

So,

A certificate is a digital document issued by a trusted third-party certificate authority (CA).

Chapter 6 Managing E-Government

E-Government implementation has to manage people, process, technology, finance and partnerships.

Approaches to Management of E-Government Systems

1. Managing Policies

E-Government sector calls for designing, promulgation, enforcement and review of a number of policies.

- **ICT Policy**- that seeks to promote the overall development of the ICT sector in the country or state.
- **E-Government policy** – that spells out the vision of e-government, the thrust areas, the prime beneficiaries and the services that are proposed to be launched in a citizen-centric way.
- **Telecom policy** – that promotes cost-effective access of the internet in a competitive environment.
- **Policy on electronic service delivery channels** – that enables setting up affordable and well - spread out facilities and mechanisms to deliver the e-services to the customers, providing them a choice of multiple channels.
- **Security Policy** – that generates the trust and confidence, which are so essential for the sustained growth of e-services.
- **PPP policy** – that promotes the forging of partnerships between the public and private sectors in their joint Endeavour to implement meaningful e-government projects.
- **An over-archiving cyber law**, together with a set of complementary Acts, which seek to regulate the various transactions of e-government.

2. Managing People

E-Government has to be designed, developed, delivered and used by people – people within government agencies, people outside the government in organizations that government would have to partner, citizen and business people. People management is difficult task because no two persons are alike and need different treatment and approach.

People management has the following:

- **Awareness Building**- evangelizing e-government and its multiple benefits among the government employees, citizens and businesses.
- **Education** of various classes of people, in the technical, legal, administrative and operational aspects of e-government besides the effective usage of the services offered by it.
- **Training** of selected categories of people in the design, development and management of e-government systems at various level of complexity.
- **Coordination** of the activities of various government agencies and NGOs.

- **Team Building** which is necessary to implement complex, business-critical systems and to sustain them over long periods.
- **Development of leadership qualities** among the key functionaries charged with the responsibilities.
- Change Management to overcome the internal and external resistance

3. Managing the Process Reform

This is the most difficult responsibility, as it involves disruption of established processes, designing innovative and integrated processes that span across agencies and, most importantly, getting people accept the new processes.

The management of e-government process reform consists of:

i. **Service Definition:** E-Government is about being service-centric. Getting definiteness and clarity in defining the set of services proposed to be targeted is an essential first step. It is necessary to conduct a research involving extensive surveys and interviews to identify the set of services that different groups within the community need. These groups could be of common citizens, business people, students, farmers, disadvantaged communities, women, children, employees etc. Redefining existing services and designing new services is the essence of a successful beginning of the e-government exercise.

ii. **BPR (Business Process Reengineering)**

This involves overcoming organizational resistance to the proposed changes, the strong forces that plead for status quo, vested interests that have hidden agenda to 'push' process that help them retain their hold and coming with an accepted set of reformed processes that best serve the interests and needs of the end users.

We need to take sufficiently motivated public servants and sensitize them on the **science of the possible**. We need to take technologists and academicians and train them on the **art of the possible**.

iii. **Legal Process Reform**

For the orderly development and sustainability of e-government initiatives, we need to bring in the necessary legal reforms. It reforms the Acts, Rules, Regulations, Forms and Procedures. The real transformation of governments can take place only by the laborious efforts in discarding old procedures, integrating processes and bringing new practices, all through statutory changes. This requires a strong team of administrative managers and management consultants work with a team of legal experts to produce simple forms and procedures drafted from the end user point of view.

iv. **Delivery Channel Reform**

The proof of e-government is in the delivery of transformed services. It is necessary to plan the establishment of delivery channels and delivery points carefully. Experts in the field of communications, digital divide and sustainable and affordable access in rural areas have to make up the delivery channel team.

4. Managing Technology

We need people who can manage technology to compliment the efforts of people who design and deploy technology. Such technology managers should find out the technological answers to the issues of translating e-government vision into reality. This involves undertaking the following tasks:

a. Design and development of architectures

We have seen the benefits of designing, developing and implementing e-government architecture in terms of long-term sustainability, interoperability and cost-effectiveness of the projects based on such architectures. We need to establish agencies at the national and state levels that can undertake this responsibility in a professional way. Such agencies should consist of individuals who have seen both sides of the coin- the government side and the technology side.

b. **Prescription of Standards**

It consists of the responsibility of developing standards for XML schemas, web services, interoperability and open standards for different technology components such as databases, hardware, communication, operating systems, open source software etc. The responsibility also extends to enforcing the prescribed standards within and across agencies.

c. Security

Promulgation of security policy and guidelines and enforcement of the same in all e-government initiatives is essential to generate the required trust and confidence among the users. Security audit is a concomitant (related) responsibility of the security organization.

d. Procurement

Very often e-government projects get bogged down at the procurement stage. It is essential to position a wing within the e-government agency, which is exclusively responsible to advice the government agencies on major procurement issues. The idea is not to centralize all procurement but to ensure that e-government procurements are done prudently, keeping the requirements of optimum utilization of assets and interoperability in view.

5. Financing e-Government Projects

Financing appraisal, financing, ROI assessment and viability studies of e-government projects involves special expertise. E-Service projects are easier to attract commercial funding. We need experts who can find innovative methods of financing e-government projects.

6. Managing Partnerships

Managing and cultivating the partnerships require expertise in the following areas:

- **Designing suitable partnerships models**

  It is necessary for governments to promote partnerships through a conscious effort by designing various partnership models and encouraging government agencies to follow them. The processes adopted to select a partner should be transparent and quick.

- **Crafting the Contracts**

  It is necessary to wary of the possible ups and downs to design the contracts that contain safety values in the event of extreme swings of the pendulum.

- **Steering the partnerships**

  Partnerships designed to provide e-government services pass through trying times especially in their relationships with the connected government agencies. This requires a steering committee for handling of situations.

E-Government Strategy

The strategy is a drill-down of the vision. It spells out, in clear terms, the manner in which the vision is sought to be realized. An e-government strategy tries to answer the basic questions that begin with 'What', 'How', 'Who' and 'When'.

An e-government strategy:

- Prepares a 'wish list' of desired outcomes in the various sectors of governance.
- Prioritizes the outcomes in the form of services and products.
- Identifies the infrastructure needs of e-government and ways to establish the same.
- Prescribes the areas in which policy, legal, administrative and process transformation are required.
- Identifies the barriers to implementation and ways to overcome them.
- Decides upon a framework for technological interventions.
- Incorporates the special needs of the socially and economically disadvantaged sections of the society.
- Lays down indicative timelines for achieving the outcomes.

An e-government strategy evolves over a period in the form of a series of approach papers and policy documents

Managing Public Data

- manage information to facilitate equality of access and promote public trust, optimize information sharing and re-use, and reduce duplication, in accordance with legal and policy obligations;
- ensure that information created, acquired, or maintained to meet program, policy, and accountability requirements is relevant, reliable, and complete;
- limit the collection, use, and disclosure of personal information to the minimum required to conduct a program or service …;
- manage information in a manner that supports the provision of services and information in both official languages …
- manage information, regardless of its medium or format, to ensure its authenticity, accuracy, integrity, clarity, and completeness for as long as it is required [by law];
- document decisions and decision-making processes throughout the evolution of policies, programs, and service delivery;
- implement governance and accountability structures for the management of information …;
- use electronic systems as the preferred means of creating, using, and managing information;
- protect essential records to ensure the continuity of key services and business operations;
- preserve information of enduring value …;
- dispose of information no longer required for operational purposes in a timely fashion;
- foster supportive environments for information management and ensure that employees meet their responsibility for managing information; and
- Assess the effectiveness and efficiency of the management of information throughout its lifecycle.

Managing Public Data

- Data quality problems can and do undermine e-government.
- Data Quality can be measured using the CARTA checklist.
- Data quality is typically addressed through general controls, which affect all e-government systems in an agency, and application controls, which relate to individual e-government systems.
- Hard solutions to public data quality problems are technology-based and fairly easy to introduce.
- Soft solutions are more difficult to implement but address more fundamental issues of human perceptions and motivations.
- Hybrid solutions combine both hard-soft and central-local components.

CARTA Indicators:

- **Completeness:** Completeness depends mainly on the source data and the process of designing data capture.
- **Accuracy:** It can help make the processing and output of information more accurate.
- **Relevance:** It makes little difference to this, since it depends on contextual issues that the technology does not affect.
- **Timeliness:** It can increase the speed with which data is input, processed and output.
- **Appropriate Presentation:** IT can improve presentation.

Hard General Controls for e-Government Data

Hard, technically oriented, rational controls are widely used in e-government systems to try to help improve data quality.

Inadequate Access Control: Unauthorized users access the public data.

Inadequate Technology Control: When the love virus hit the US government in 2000.

When Application Controls are missing in public data: Number of duplicate data had been inserted.

Soft Solutions to Public Data Quality Problems:

- Ensure there is a user.
- Merge stakeholder roles.
- Make early stakeholders into data users.
- Other feedback to early stakeholders.
- Other reward and punishment techniques.
- Find alternatives sources.

Hybrid Data Control Mechanism:

Public managers must adopt not just the easy hardware solutions, but also soft solutions. They also need to adopt a set of hybrid solutions that sit at the interface between people and technology: representing the socio-technical component of hybrid approaches.

- Policy development and dissemination.
- Password Update
- Data backup
- Repair and Maintenance
- Insurance
- Bans
- Careful use of technology

ISSUES IN E-GOVERNANCE

A. Technical Issues

i. **Interoperability:** The interoperation of various state governments, the various ministries with in a state government is a critical issue. Integration of data is main problem, how to capture the data in web based form and how to transfer it in common format for processing and sharing the information.

ii. **Privacy:** privacy of any transaction or information provided by the citizen to the government agency must be ensured. Otherwise the information can be misuse by the private sector or competitors and the users may be reluctant to access the services provided.

iii. **Security:** Transaction security is another major problem in e-governance. The tax, fine and bill payment must be secured and the system design should be full proof.

iv. **Authentication:** The authentication of citizens requesting services needs to be verified before they access or use the services. The digital signature plays an important role in providing the authenticity but this is expensive and requires frequent maintenance.

B. Economic Issues

i. **Cost:** Implementation, operations and maintenance cost of service provided should be low enough for high cost benefit ratio.

ii. **Maintainability:** It has been continuously evolving and software is frequently upgraded. Thus the system must be compatible and maintainable for easily fulfillment of emerging needs.

iii. **Reusability:** E-governance should be considered as nationwide plan and the implemented modules must be reusable by other administrations.

iv. **Portability:** The primary requisite for portable applications is independence of components from hardware or software platforms, to help in possible reuse by other administrations.

C. Social issues

i. **Accessibility:** E-governance service should be accessible for anybody from anywhere at any time. Even if internet population is growing exponentially, there is a very big portion of the population who may not able to access e-governance for various reasons.

ii. **Usability:** All the users may not be expert of ICT transactions or the technology used for e-governance. Therefore the service provided must be usable or user friendly. To make the system usable, the guidance of operation may be provided to the users.

iii. **Acceptance:** E-governance requires reconfiguration of internal and external structure of public sectors. The main aim is to improve the system efficiently and to provide high quality services to the citizens. E-governance is for citizen convenience, instead of convenience of government. The power conflicts over the departmental and functional boundaries become more prominent in integration process.

iv. **Use of local languages:** The access of information must be permitted in the local languages for user comfort. There should be language software or some other technologies to translate the information from English to local languages.

v. **Awareness in rural areas:** In Nepal, there are very high percentage of villages where awareness of e-governance is required since large portion of rural populations are not aware of new technologies and computer educations.

Emerging Management Issues for E-Government

- Performance Management
- Performance Indicators
- Measurement of Performance
- Policies on Public Data
- Access Policies for Management of Data Records
- Access Policies for Freedom of Information
- Access Policies and the Digital Divide
- Policies on Other Issues

Performance Management

- Technique originated in the private sector and is being promoted in the public sector
- Follows a standard pattern of target setting, measurement, evaluation and control
- Performance should be measurable
  - Subjective, qualitative assessments will be conflicting
  - Measures should be valid, relevant and valuable
- Public Sector uses public-private hybrid recommendations
- Reward the good and rectify bad performance
  - One-off payments for achieving particular targets, gain sharing and still pay etc.
  - Non-financial rewards, such as performance wards, personal recognition, from senior staff
  - Use punishment, but with great care. Avoid financial penalties and avoid punishing occasional mistakes.

Performance Indicators

- Three main focal points for performance indicators
  1. Input: These are typically seen as IT measures that are independent of client
  2. Output: These are typically seen as information services measures, since they relate to the service as it is received and used by clients.

3. Outcome: These are typically seen as business process measures, since they related to client processes that the IS/IT function supports

- Public agencies are now moving on to outcome measures as it focuses on the actual use and its impact of the process

Measurement of Performance

- How are the performance indicators described above actually measured?
  1. Internal subjective: The measures are based on the judgment of internal clients, such as customer satisfaction rating scales
  2. Internal Objective: The measures are based on objective quantification within the organization like the number of job seekers who were put into work by a call centre
  3. External: The measures are based on quantification from outside the organization like external auditing, benchmarking etc.
- There has been a tendency to move up the scale over time, with a growth in the external measures.

Control of Performance

- Means of affecting performance through control measures could be
  1. Provider management control: Managers within the IS/IT service provider are responsible for managerial rewards and remedial measures
  2. Client management control: Managers within the IS/IT service client are responsible for managerial rewards and remedial measures
  3. Client financial control: Managers within the Is/IT service client are responsible for financial rewards and remedial measures
- Hybrid financial control arrangements are used by public agencies
  - Gain sharing, Efficiency dividends, Performance budgeting etc.

Policies on Public Data

- Public agencies operate in a sea of government laws, policies and regulations
- It pressurize agency managers to develop and implement internal policies
- The issues also relate to policies on the management of public data. **Eg. Access-Income Barrier**
- Court documents in the public domain are digitized
- Aim is to make the access easier and cheaper, but
- Financial pressures on departments to recover costs and maximize returns on their information/data
- It leads to controls and charging for accessing data
- The more the government charges for its data, the grater the barriers for accessing the information

Management of Data Records

- Digital information lasts forever or five years-whichever comes first
- There are two main issues in creating policies for data access
    - Storage and Retrieval
- Public servants are not yet attuned to electronic records management
    - Engage in wholesale deletion or over-writing of government records
- Archivists must either maintain large quantities of increasingly obsolete equipment, Or
- Copy and recopy ever-larger amounts of data onto new formats
- These electronic files must then be held securely
    - Documentation describing how the records were created is necessary

Access Polices for Freedom of Information and Issues

1. **Procedures:** Clarifying how citizens/businesses can obtain data direct without requests or how information requests are to be made
2. **Data Management:** Ensuring that the type of back-office, records and data management procedures are followed so that data and records can be located in a timely and cost-efficient manner
3. **Performance measures:** Setting out performance indicators for FOI response service
4. **Charges:** Determining a reasonable level of charges to be levied for searches and copying; putting a billing and payment system in place
5. **Appeals:** Setting in place an appeals procedures to appeal against problems with performance, charges or denial of access

Access Policies and the Digital Divide

- Downloading a government report via the internet or buying paper version, which is cheaper?
- IT has made it cheaper and easier to access data
    - To get that far you need an IT infrastructure in place first
- IT raises barriers and has created a digital divide, how?
    - For IT-based data, computer literacy is necessary and not everyone has those skills
    - One group reaps the benefits of IT-enabled accessibility while the other group cannot
- Governments and agencies are putting in place a variety of access policies to overcome these use inequalities
- This aims to increase access to data and bring other perceived benefts of access to IT
- Some initiatives have focused on increasing ownership
    - Full payments or subsidies as ways to increase the numbers of those who actually own computers

- Governments may set up initiatives for increasing access to IT that is government or community-owned IT centers
- These centers should have IT facilitator to help people learn

Privacy Policy for Data Protection

- Data Protection legislation chimes very much with information resource management principles
- Identify someone senior and central responsible and accountable for the accessibility and confidentiality of data held
- Public web sites should incorporate privacy principles and privacy statements that detail how a site collects data; how that data is used and who the data is shared with
- Reflecting the access-privacy tension, restrict agency activity particularly setting limits on data like national security

Security Policies for Protection of Data

- Security may be in tension with goals of access and income
- Use of web sites within e-government systems is followed by the rise in global terrorism and high profile cyber crimes
- Data security policies are typically based on
    - Risk assessment and mitigation approach
- Institutional mechanisms such as the government-wide IT security Offices to drive implementation of policies is also emerging

Elements of the Data Security Policy

- **Incident reporting:** Reporting of data security incidents both within and outside the agency
- **Review:** Of data security policies to ensure they are working as intended
- **Collaboration:** Working with the private sector on areas of critical data infrastructure, and sharing of knowledge and warnings
- **Continuity:** Additional emphasis on robust contingency planning to ensure fallbacks in case key e-government systems are attacked
- **Intelligence:** Greater efforts to identify sources of data attacks

Policies on Other Issues

- There are other policy issues of relevance to e-government
- Disability / Accessibility
    - New technology offers ways to overcome some of the barriers faced by people with disabilities

        - To reduce discrimination, a number of countries have introduced anti-discriminatory legislation
        - To comply with the legislation, managers have been introducing in-house policies covering the development of IS
- There are different types of technology to help with disabilities

Types of Technology

- **Software**: Most of the specifications for software pertain to usability for people with vision impairments.
- **Web sites:** Ensuring access for people with vision impairments who rely on various assistive products to access computer-based information
- **Telephones**: Designed primarily to ensure access to people who are hard of hearing
- **Multimedia**: For example captioning of video
- **Computers:** Must allow non-keyboard forms of data entry, and alternative mechanisms for data output
- Policy requirements that relate to accessibility fall into two main types
    - First, there are very specific guidelines, such as those provided for e-Government web sites design
    - Second, there is a set of higher-level issues
        - **Structures:** A designated agency official responsible for accessibility policies, processes and structures
        - **Systems:** Processes and structures for feedback on accessibility, and email contact and a system for complaints and for dispute resolution
        - **Processes:** Training of staff to raise accessibility awareness and skills; ensuring procurement of compliant technology

Ergonomics

- Ergonomics means using knowledge of humans' physical and psychological characteristics to design and implement technology
- Applying ergonomics in the design of e-government systems can
    - Reduce the health problems and increase the efficiency
- Health problems have been associated with computing
    - Physical symptom is generally seen as Repetitive Strain injury (RSI)
    - This is damage that occurs through the heavy repetive use of particular muscles
- Realization about IT-related health problems, has led to its legislation

Standardization for Ergonomics

- **Equipment**: adjustability and clarity of monitors; keyboard design and adjustability; adjustability of work surfaces, chairs and footrests;

- **Work environment:** space, light, reflection, noise, heat and radiation; and software interface: ease of use, nature of human-computer interaction
- Stress can arise from problems with the physical environment but tends to arise more from the general arrangement and organization of work in IT
- Attend not just to the technical issues such as lighting and positioning, but also to people-related issues such as consultation and job design structure
- Second, we should balance the interests of different stakeholders
- Focus on interests of external stakeholders and also the agency staff

Immerging Management Issues for E-Government

The implementation of e-governance system has many aspects. For e.g. normally e-governance services are non-profit making services and most of the time, their payback period is very high which makes them capital intensive. The 7-C model appropriately indicates various implementation aspects of e-governance. The 7-Cs are:

1. **Capital:** E-governance services meant for providing faster and effective services to the citizens and profit considerations are not very prominent aspect of these services. Many services which were implemented long ago are yet to break even due to high cost. The operational cost with a subsidy to users makes it tough to generate operational profit.
2. **Connectivity:** Success of e-governance service depends on its reach to the people. A good system can be good, only when it can benefit a large section of the connectivity till the last mile.
3. **Commitment:** As e-governance is no viewed in terms of accounting profits and shorter payback period and even one of the great motivators, money, is absent, it is at the different hierarchy of the system. It is needed to push, through the project, to its logical end.
4. **Competence:** Competence is required to gather the intelligence at the grass root level. Understanding of people's problem as well as those who are going to provide e-governance services (mainly operators and clerks) needs more than understanding of software engineering.
5. **Content:** In India the lack of customized content is one of the hurdles in implementation of the e-governance services. The content is not available in local language, which can capture understanding of people at the gross root level.
6. **Citizen Interface:** Interface should be illustrative and easy-navigating, so that even native users do not find it tough to avail of the services.
7. **Cyber laws:** Services should be backed by cyber laws to make the documents or information legally valid. Indian IT act 2002 was one of the endeavors towards this, which made e-mails and other digital documents as valid as a legal documents.

E-GOVERNANCE EVOLUTION IN INDIA: CHALLENGES BEFORE STAKEHOLDERS

1. Lack of IT literacy and awareness regarding benefits of e-governance: There is general lack of awareness regarding benefits of e-governance as well as process involved in implementing successful G2G, G2C, G2B projects. The administrative structure is not geared for maintaining, storing and retrieving the governance information electronically.
2. Urbanization of existing ICT infrastructure: To a larger extend, the computers in the department are used for the purpose of word processing only. This is resulting in the underutilization of computers in terms of their use in data mining for supporting management decisions. The time gap between the procurement of the hardware and development of custom applications is so large that by the time application is ready for use, the hardware becomes obsolete.
3. Attitude of government departments: The Psychology of government servants is quite different from that a private sectors. Thus any effort to implement Database Management System and workflow technologies or bringing out change in the system is met with the resistance from the government servants.
4. Lack of coordination between government department and solution developers: Designing of any application requires a very close interaction between the government department and the agency developing the solutions. Consequently the solution developed and implemented does not address the requirements of an e-governance project and hence does not get implemented.
5. Resistance to re-engineering of departmental processes: Successful implementation of e-governance project requires a lot of restructuring in administrative processes, redefining of administrative procedures and formats which finds the resistance in almost all the departments at all the levels. The content collected or maintained by various e-governance portals in unreliable or full of gaps. It is difficult for any e-governance solution to achieve its intended results.
6. Lack of infrastructure for sustaining e-governance projects at national level: Infrastructure to support e-governance initiatives does not exist within government departments. The infrastructure creation is not guided by a uniform national policy, but it dependent on the needs of individual officers championing a few projects. Therefore, the required networking and communication equipment is either nonexistent in government departments or if it exists at all, it does not serve any tangible purpose as per the requirement of e-governance project is concern.

SUGGESTIONS FOR SUCCESS OF AN E-GOVERNANCE

For success of an e-governance and superior service delivery, it is imperative that the government agency focuses on whole citizen experience. The government agency needs to integrate information from all points of citizen integration. The e-governance applications that are emerging as islands of success have to be interoperable. Following are some suggestions for the successful transformation.

1. Create literacy and commitment to e-governance at high level: The most important requirement in e-governance is a training program for policy makers, politicians and IT task force members. The training program needs to be focused according to the requirements of the policy makers at the top.
2. Conduct usability surveys for assessment of existing e-governance projects: There is a varying degree of development of e-governance among the different states. A few states have leapfrogged into a digital era, whereas a few are yet to start with any initiative. Therefore an awareness exercise should be carried out in all state government departments, to understand their level of acceptability of the e-governance.
3. Starting with implementation of pilot projects and replicating the successful ones: The pilot projects taken in various states should be accessed for their achievement levels. They should be classified as success or failure according to the desired output written down before implementation of the projects. The successful projects should be replicated over the nation with members drawn from the implementing team. The projects, which could not achieve the desired outcome, should be documented for possible causes of failure.
4. Follow the best practices in e-governance: The study of the best practices will bring forward the best practices followed nationally and internationally. The national and international beat practices study will give a great momentum to the process of e-governance.
5. Build nation resource database of e-governance projects: This would allow any organization planning an IT project to instantly ascertain whether any such project has already been implemented anywhere in the country. And intending implementers would know who the people in similar projects are and how to reach them.
6. How clearly defined interoperability policy: The e-governance architecture needs to ensure that the components are scalable and adaptable to the future requirements. It has also to ensure that the local architecture fits into state level and the same into national and global architecture. Interoperability is a major criteria while defining the architecture.
7. Manage and update content on government websites efficiently and regularly: Content is the 'heart' of any IT project. The process of content development encompasses a whole range of activities starting with a comprehensive study of the system and identification of the objectives. It ends up with delivery of the intended benefits to the citizens or other users of the system. The government agencies must ensure that the data on the sites is always updated and relevant.