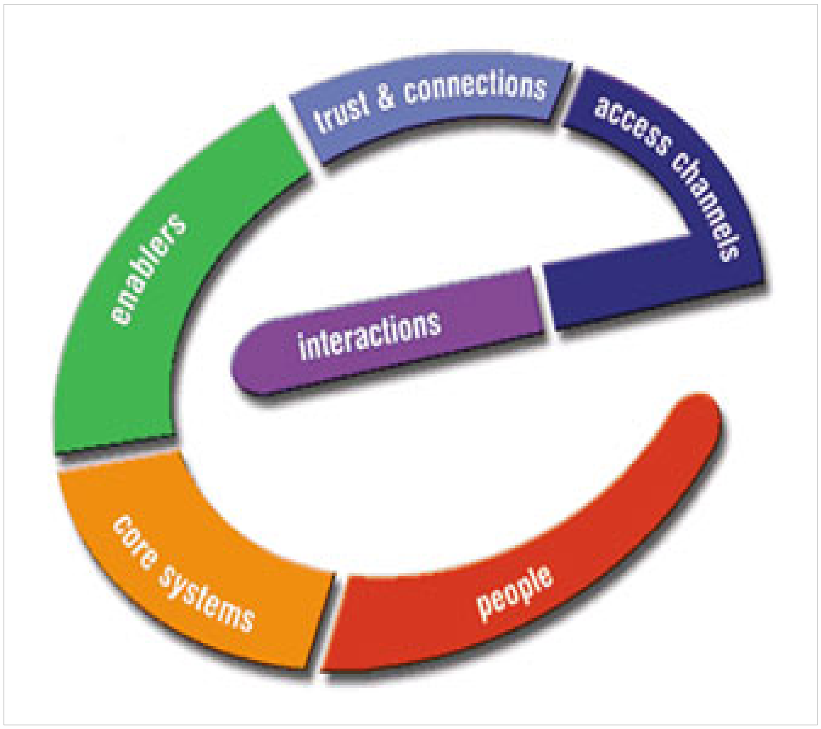
यशवंतराव चव्हाण विकास प्रशासन प्रबोधिनी
(महाराष्ट्र शासनाची अंगीकृत संस्था)

Yashwantrao Chavan Academy of Development Administration
(A Government of Maharashtra Organisation)

Reading Material
for
# e-Governance Training Sessions



Yashwantrao Chavan Academy of Development Administration (YASHADA)
Rajbhavan Complex, Baner Road, PUNE - 411 007, Maharashtra
Telephone : 020-25608277 | Fax : 020-25608100 | E-mail: contact@yashada.org | Website: http://www.yashada.org

Acknowledgements and Disclaimer

This reading material is a compilation of internal knowledge base and content from various other sources, particularly from NISG, DEITY (Government of India), Department of Information Technology, Government of Maharashtra, and e-Governance Standards websites. Yashwantrao Chavan Academy of Development Administration (YASHADA) duly and thankfully acknowledges the respective sources.

The aim of this reading material is to provide a preliminary understanding on the subjects and areas covered as part of the e-Governance training programs. For undertaking any e-Governance related activities in the areas covered under the training program, this document should be treated only as a quick reference on the topics, and should not be treated as a guideline and / or instructions for undertaking the activities covered under the e-Governance projects. It is expected to provide useful learning for officials working in the area of e-Governance.

The document by no means has any commercial intention and is solely compiled for the purpose of knowledge sharing. It is meant for free of cost distribution amongst participants of YASHADA's various e-Governance training programs.

YASHADA shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretation thereof. The reader is solely responsible for the selection of this material to achieve its intended results.

The content provided herein is subject to change without prior notice.

How to use this Reading Material

This compilation on e-Governance is aimed primarily for the officials in Government of Maharashtra departments who are responsible for, or are associated with, managing various e-Governance projects in their departments. It is also a compendium of information from diverse sources which will be invaluable to the readers from both ICT and non-ICT background as a quick reference guide on various e-Governance concepts covered during the training program. This document is intended to be treated as a quick reference guide.

This reading material is organized into 22 chapters and 2 Annexures. Each chapter presents information for readers with different levels of technical expertise and differing needs. At the start of each section is a layman's introduction to the techniques, concepts or processes being covered during the training program. This provides a concise background to the topic then gives an intuitive discussion of the concepts, objectives and practical importance of the techniques in non-technical language. These introductions are likely to be all that a decision maker, project manager or any other officer in charge of the e-Governance Project might need to gain a preliminary knowledge of the key issues. For those readers with greater technical involvement, they provide a clear overview of the topic and indications of further sections that may be advantageous or necessary to study.

Flow diagrams, tables, graphics and images are used extensively to facilitate easy comprehension and quick recollection of the topics covered therein. A list of relevant websites and further reading resources that can be visited / referred in conjunction with the topics covered is provided in the last chapter.

e-Governance, as a subject, is evolving rapidly but we hope that this reading material provides a concise, informative and easily used companion for those involved in e-Governance Projects, so that they can use the topics covered under the training to their full advantage.

Feedback from the readers of this document will be of a great help to us in improving it further in its future editions.

Contents at a Glance

Contents

1. Introduction

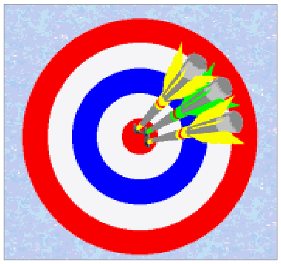
1.1 Introduction to the Course

The "e-Governance Project Lifecycle" course is designed to equip participants with the necessary background and understanding on structured approach for conceptualization of e-Governance initiatives, various phases of e-Governance project Lifecycle, key considerations during each phase of development, activities and outputs of each phase etc. The training course will equip the participants with a range of emerging practices and examples of how e-Government and e-business services can be undertaken by government/public sector organizations to strategically plan and transform their organization to:

- Realign government service delivery with the citizen focus
- Improve transparency, accountability and trust in the government
- Improve the citizen experience in Government transactions, reducing time, costs and administration burden for government agencies

1.2 Enabling Objectives of the course

The training course performance objectives in terms of expected capabilities to be demonstrated by the participants in their respective departments post training completion include the following:



- Support the government departments, in terms of leading or being part of team responsible for, e-Governance project Conceptualization and design
- Support the government departments in effectively planning and managing various phases of e-Governance project development and implementation
- Leverage the strengths of private sector in e-Governance initiatives through effective procurement approach and manage service delivery throughout project Lifecycle
- Application of learning and good practices in e-Governance projects implementation to minimize the learning curve and to maximize the benefits for the department

1.3 Knowledge, skills and attitudinal development objectives in the course

Following summarizes the key Knowledge, Skills and Attitude development focus areas under this course.

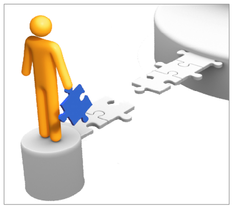
Knowledge

- Need for change in current service delivery model and role of e-Governance
- National e-Governance Plan, MMPs, institutional structures and related policies

- e-Governance evolution model and approach for implementation of e-Governance
- Lifecycle and phases, scope, approach and deliverables in each phase in e-Governance project development and implementation
- Approach for addressing project requirements during the Lifecycle
- Role for private sector participation.
- Capacities and resources required for e-Governance implementation
- Policy and legislative framework support for e-Governance

Skills

- Use ICT and allied tools for increasing office productivity
- Employ ICT in e-Governance and services delivery
- Employ Regional Language(s) in computing
- Deploy anti-threat measures in their ICT infrastructure
- Play a key role in capacity building of colleagues and subordinates



Attitude

- Recognize the need for change and transformation in administration
- Appreciate the role of e-Governance and IT in government administration
- Recognize the need for structured and holistic approach for e-Governance implementation than mere computerization
- Appreciate the private sector participation and potential in government transformation
- Recognize the need for managing the change effectively in the organization

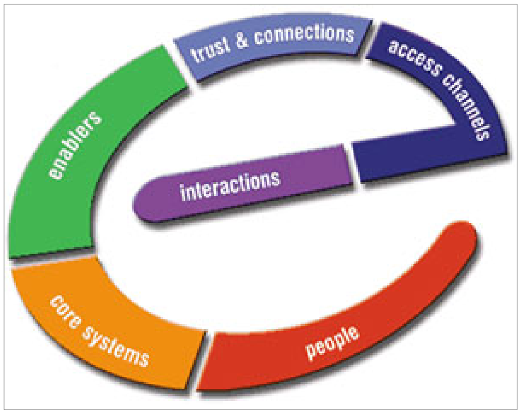
मनोवृत्तीवरच
अवलंबून
सर्वकाही

2. Introduction to e-Governance

In India, the government deals with several matters affecting people's lives. It is said government is all encompassing as it touches the lives of human beings from cradle (health services for women and children) to grave (payment of pensions, gratuity etc.).

Government has to tackle unending problems and challenges emanating from over-population, poverty, illiteracy, unemployment and underdevelopment.

Government is expected to look after defense, foreign policy, communications and infrastructure, maintenance of land records, maintenance of law and order, collection of revenue, promotion of agriculture, science and technology, international trade, banking, insurance, transport, social welfare, family planning etc.

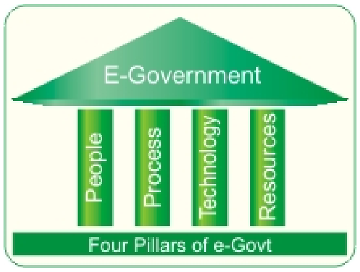


As citizens of India, we have to deal with government in our day-to-day lives. Citizens expect speedy service, courteous treatment, and quick disposal of grievances or applications. This interaction, however, is not always pleasant. The general perception among citizens is that the quality of administration is deteriorating day-by-day and that quality of governance needs to be considerably improved upon. The general feeling outside the government is that the government is huge, it lacks direction, it is unmanageable, is wasteful and it is uncaring of the citizen. But those in the government continue to feel that they are doing a fine job and nothing could be done better. There is, therefore, a wide gap between the expectations of the citizens and their experience with the government. This gap can only be filled by drastic simplification of procedures and change in attitude of civil servants vis-a-vis the citizens.

Just as business corporations have discovered over the last few decades that information technology can make their service (or product) delivery value chain more efficient and lead to quality improvements and cost savings, governments in developing countries, over the last 5-7 years, have discovered that information technology can make the provision of services to the citizen more efficient and transparent, can save costs and lead to a higher level of comfort and satisfaction to the citizens in dealing with Government.

So far as governments are concerned, the coming together of computerization and internet connectivity/web-enablement in association with process Re-engineering, promises faster and better processing of information leading to speedier and qualitatively better decision making, greater reach and accountability, better utilization of resources and overall good governance. In the case of citizens, it holds the promise of enhanced access to information and government agencies, efficient service delivery and transparency in dealings and interactions with government.

With the increasing awareness among citizens about their rights and the resultant increase in expectations from the government to perform and deliver, the whole paradigm of governance has changed. Government, today, is expected to be transparent in its dealings, accountable for its activities and faster in its responses. This has made the use of ICT imperative in any agenda drawn towards achieving good governance. It has also led to the realization that such technologies could be used to achieve a wide range of objectives and lead to faster and more equitable development with a wider reach.



2.1 Concept and definition of e-Governance

The "e" in e-Governance stands for 'electronic'. Thus, e-Governance is basically associated with carrying out the functions and achieving the results of governance through the utilization of what has today come to be known as ICT (Information and Communications Technology). The reason why countries around the world are increasingly opting for 'e-Governance' is that governance per se has become more complex and varied in the last few decades and more importantly, citizens' expectations from government have increased manifold. ICT facilitates efficient storing and retrieval of data, instantaneous transmission of information, processing information and data faster than the earlier manual systems, speeding up governmental processes, taking decisions expeditiously and judiciously, increasing transparency and enforcing accountability. It also helps in increasing the reach of government - both geographically and demographically.

The primary purpose of governance is the welfare of citizens. While one aspect of governance relates to safeguarding the legal rights of all citizens, an equally important aspect is concerned with ensuring equitable access to public services and the benefits of economic growth to all. It is expected that e-Governance would enable the government to discharge its functions more effectively. However, this would require the government to change itself - its processes, its outlook, laws, rules and regulations and also its way of interacting with the citizens. It would also require capacity building within the government and creation of general awareness about e-Governance among the citizens.

During the initial stages of introduction of ICT in governance there was resistance from some quarters. Some felt that computerization cannot work in the complex government system and that introduction of computers would lead to un-employment. There were also serious doubts whether government employees at all levels would be able to handle computers. Fortunately all these misgivings have proved wrong. Today, new software tools have enough flexibility, to accommodate the most complex situations. The new technology makes the machine-human interface very user-friendly. The Information Technology (IT) and Information Technology Enabled Services (ITES) sectors have created millions of jobs besides improving vastly on the services provided by government undertakings like Banks, Airlines, Railways, etc. Thus e-Governance is no longer a far-fetched dream. In fact, for a Government in a country like India - with 1.2 billion population, more than 600,000 villages, growing economy coupled with increasing aspirations of the citizens for better quality of life - use of Information Technology in improving government processes has not just become vital but essential and without which it would be extremely difficult, if not impossible, to serve its citizens efficiently and transparently and ensure participation of larger number of people in decision making at all levels of Government - Centre, State and local.

e-Governance is, in essence, the application of Information and Communications Technology to government functioning in order to create 'Simple, Moral, Accountable, Responsive and Transparent (SMART) governance. This would generally involve the use of ICTs by government agencies for any or all of the following reasons:

- Exchange of information with citizens, businesses or other government departments
- Speedier and more efficient delivery of public services
- Improving internal efficiency
- Reducing costs / increasing revenue
- Re-structuring of administrative processes and improving quality of services

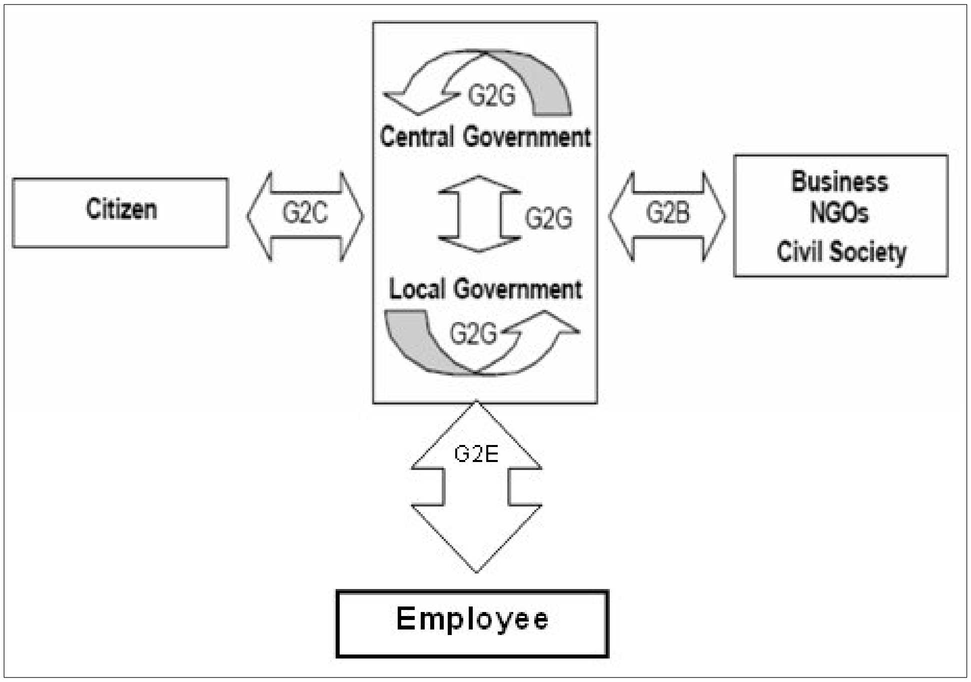
Although the term 'e-Governance' has gained currency in recent years, there is no standard definition of this term. Different governments and organizations define this term to suit their own aims and objectives. Sometimes, the term 'e-Government' is also used instead of 'e-Governance'.

e-Governance aims to make the interaction between government and citizens (G2C), government and business enterprises (G2B), and inter-agency relationships (G2G) more friendly, convenient, transparent, and inexpensive.

The goals of e-Governance are:

- Better service delivery to citizens
- Ushering in transparency and accountability
- Empowering people through information
- Improved efficiency within Governments
- Improve interface with business and industry

e-Governance facilitates interaction between different stake holders in governance using ICT (indicated by block arrows in the diagram below).



Interactions between main groups in e-Governance

These interactions may be described as follows:

- **G2G (Government to Government)** - In this case, Information and Communications Technology is used not only to restructure the governmental processes involved in the functioning of government entities but also to increase the flow of information and services within and between different entities. This kind of interaction is only within the sphere of government and can be both horizontal i.e. between different government agencies as well as between different functional areas within an organization, or vertical i.e. between national, provincial and local government agencies as well as between different levels within an organization. The primary objective is to increase efficiency, performance and output.
- **G2C (Government to Citizens)** - In this case, an interface is created between the government and citizens which enables the citizens to benefit from efficient delivery of a large range of public services. This expands the availability and accessibility of public services on the one hand and improves the quality of services on the other. It gives citizens the choice of when to interact with the government (e.g. 24 hours a day, 7 days a week), from where to interact with the government (e.g. service centre, unattended kiosk or from one's home/workplace) and how to interact with the government (e.g. through internet, fax, telephone, email, face-to-face, etc). The primary purpose is to make government, citizen-friendly.
- **G2B (Government to Business) -** Here, e-Governance tools are used to aid the business community - providers of goods and services - to seamlessly interact with the government.

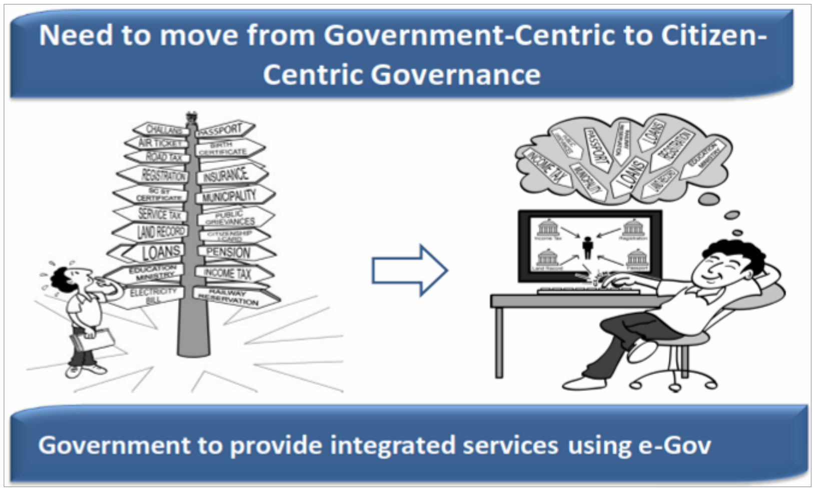
The objective is to cut red tape, save time, reduce operational costs and to create a more transparent business environment when dealing with the government. The G2B initiatives can be transactional, such as in licensing, permits, procurement and revenue collection. They can also be promotional and facilitative, such as in trade, tourism and investment. These measures help to provide a congenial environment to businesses to enable them to perform more efficiently.

- **G2E (Government to Employees) -** Government is by far the biggest employer and like any organization, it has to interact with its employees on a regular basis. This interaction is a two-way process between the organization and the employee. Use of IeT tools helps in making these interactions fast and efficient on the one hand and increase satisfaction levels of employees on the other.

2.2 Benefits and outcomes of e-Governance

e-Governance is about reforms in governance, facilitated by the creative use of Information and communications Technology. The following can therefore be achieved as a result of e-Governance:

- **Better access to information and quality services for citizens:** IeT would make available timely and reliable information on various aspects of governance. In the initial phase, information would be made available with respect to simple aspects of governance such as forms, laws, rules, procedures etc later extending to detailed information including reports (including performance reports), public database, decision making processes etc. As regards services, there would be an immediate impact in terms of savings in time, effort and money, resulting from online and one-point accessibility of public services backed up by automation of back end processes. The ultimate objective of e-Governance is to reach out to citizens by adopting a Lifecycle approach i.e. providing public services to citizens which would be required right from birth to death.



Need to move from Government-Centric to Citizen-Centric Governance

Government to provide integrated services using e-Gov

- **Simplicity, efficiency and accountability in the government:** Application of IeT to governance combined with detailed business process Re-engineering would lead to simplification of complicated processes, weeding out of redundant processes, simplification in structures and changes in statutes and regulations. The end result would be simplification of the functioning of government, enhanced decision making abilities and increased efficiency across government - all contributing to an overall environment of a more accountable government machinery. This, in turn, would result in enhanced productivity and efficiency in all sectors.
- **Expanded reach of governance:** Rapid growth of communications technology and its adoption in governance would help in bringing government machinery to the doorsteps of the citizens. Expansion of telephone network, rapid strides in mobile telephony, spread of internet and strengthening of other communications infrastructure would facilitate delivery of a large number of services provided by the government. This enhancement of the reach of government - both spatial and demographic - would also enable better participation of citizens in the process of governance.
- **Enabling Environment for Promoting Economic development** - Technology enables governments to create positive business climates by simplifying relationships with businesses and reducing the administrative steps needed to comply with regulatory

obligations. There is a direct impact on the economy, as in the case of e-procurement, which creates wider competition and more participants in the public sector marketplace.

- **Enhancing Transparency and Accountability:** e-Governance helps to increase the transparency of decision-making processes by making information accessible – publishing government debates and minutes, budgets and expenditure statements, outcomes and rationales for key decisions, and in some cases, allowing the on-line tracking of applications on the web by the public and press.
- **Improving Service Delivery**: Government service delivery, in the traditional process, is time consuming, lacks transparency, and leads to citizen and business dissatisfaction. By putting government services online, e-Governance reduces bureaucracy and enhances the quality of services in terms of time, content and accessibility through integrated service delivery platforms at the door steps of citizen.
- **Improving Public Administration**- e-Governance administrative components, such as a computerized treasury, integrated financial management information systems, and human resource management systems, lead to greater efficiency in public administration. Features include the integration of expenditure and receipt data, control of expenditure, human resources management, intelligent audit through data analysis and the publishing of financial data.

2.3 e-Governance maturity model

In order to guide and benchmark e-Governance development, various e-Governance development models, so called maturity models have been developed. These models outline various stages for e-Government development.

Most widely accepted among these models is the "Gartner e-Governance Maturity Model". The maturity model, comprises of four phases, namely Information, interaction, transaction and transformation. In each of the four phases, the delivery of online services and use of ICT in government operations serve one or more of the aspects of e-Governance: democracy, government, business.

Description of each of the phases is as follows:

Information: In the first phase e-Governance means being present on the web, providing the external public (G2C and G2B) with relevant information. The value to the public is that government information is publicly accessible; processes are described and thus become more transparent, which improves democracy and service.

Internally (G2G) the government can also disseminate information with static electronic means, such as the Internet. In this phase it is all about information.

Interaction: In the second phase the interaction between government and the public (G2C and G2B) is stimulated with various applications. People can ask questions via e-mail, use search engines for information and are able to download all sorts of forms and documents. These functionalities save time. In fact the complete intake of (simple) applications can be done online 24/7. Normally this would have only been possible at a counter during opening hours.

Internally (G2G) government organizations use Local Area Networks (LAN), intranets and e-mail to communicate and exchange data. The bottom line is that more efficiency and effectiveness is achieved because a large part of the intake process is done online. However, you still have to go to the office to finalize the transaction, by paying a fee, handing over evidence or signing papers.

Transaction: With phase three the complexity of the technology is increasing, but customer (G2C and G2B) value will also be higher. Complete transactions can be done without going to an office. Examples of online services are filing income tax, filing property tax, extending/renewal of licenses, visa and passports and online voting. Phase three is mainly complex because of security and personalization issues - e.g., digital (electronic) signatures are necessary to enable legal transfer of services. In this phase, internal (G2G) processes have to be redesigned to provide good service. Government needs to create new laws and legislation that will enable paperless transactions with legal certification. The bottom line is that now the complete process is online, including payments, digital signatures etc. This saves time, paper and money.

Transformation: The fourth phase is the transformation phase in which all information systems are integrated and the public can get G2C and G2B services at one (virtual) counter. One single point of contact for all services is the ultimate goal. The complex aspect in reaching this goal is mainly on the internal side, e.g. the necessity to drastically change culture, processes and responsibilities within the government institution (G2G). Government employees in different departments have to work together in a smooth and seamless way. In this phase cost savings, efficiency and customer satisfaction are reaching highest possible levels.

The UN e-Governance Survey 2008 report has taken this model a step further and introduced, as fifth phase, the concept of 'Connected Government', which means Governments transform themselves into a connected entity that responds to the needs of its citizens by developing an integrated back office infrastructure. This is characterized by:

1. Horizontal connections (among government agencies)
2. Vertical connections (central and local government agencies)
3. Infrastructure connections (interoperability issues)
4. Connections between governments and citizens
5. Connections among stakeholders (government, private sector, academic institutions, NGOs and civil society)

2.4 Evolution of e-Governance in India

Recognizing the increasing importance of electronics, the Government of India established the Department of Electronics in 1970. The subsequent establishment of the National Informatics Centre (NIC) in 1977 was the first major step towards e-Governance in India as it brought 'information' and its communication in focus. In the early 1980s, use of computers was confined to very few organizations. The advent of personal computers brought the storage, retrieval and processing capacities of computers to Government offices. By the late 1980s, a large number of government officers had computers but they were mostly used for 'word processing'. Gradually, with the introduction of better software, computers were put to other uses like managing databases and processing information. Advances in communications technology further improved the versatility and reach of computers, and many Government departments started using ICT for a number of applications like tracking movement of papers and files, monitoring of development programs, processing of employees' pay rolls, generation of reports etc.

However, the main thrust for e-Governance was provided by the launching of NICNET in 1987 - the national satellite-based computer network. This was followed by the launch of the District Information System of the National Informatics Centre (DISNIC) program to computerize all district offices in the country for which free hardware and software was offered to the State Governments. NICNET was extended via the State capitals to all district headquarters by 1990.

In the ensuing years, with ongoing computerization, tele-connectivity and internet connectivity, came a large number of e-Governance initiatives, both at the Union and State levels. A National Task Force on Information Technology and Software Development was constituted in May 1998, while recognizing Information Technology as a frontier area of knowledge per se, it focused on utilizing it as an enabling tool for assimilating and processing all other spheres of knowledge. It recommended the launching of an 'Operation Knowledge' aimed at universalizing computer literacy and spreading the use of computers and IT in education. In 1999, the Union Ministry of Information Technology was created. By 2000, a 12-point minimum agenda for e-Governance was identified by Government of India for implementation in all the Union Government Ministries/Departments. Some of the important agenda points included the following actions to be taken by the Ministries / Departments:

a) Each Ministry/Department must provide pCs with necessary software up to the Section Officer level. In addition, Local Area Network (LAN) must also be set up.

b) It should be ensured that all staff who have access to and need to use computer for their office work are provided with adequate training. To facilitate this, inter alia, Ministries/Departments should set up their own or share other's Learning Centres for decentralized training in computers as per the guidelines issued by the MIT.

c) Each Ministry/Department should start using the Office Procedure Automation software developed by NIC with a view to keeping a record of receipt of dak, issue of letters, as well as movement of files in the department.

d) Payroll accounting and other house-keeping software should be put to use in day-to-day operations.

These initiatives / actions though served an important purpose in introducing ICT in Government but fell far short of expectations because the approach was still Departmental and not Citizen- centric. Citizens did not benefit much as they still were supposed to physically go to each Department (or its associated office) to avail the service. Second, there was no integration of information within and among departments. This resulted in creation of silos of information. Third, from a government perspective, there was huge duplicity of effort and wastage of precious resources in creation of overlapping infrastructure by each Department / Ministry at the Central and State level.

Prior to 2006 when the Government of India formally launched its National e-Governance Plan (NeGP), which is discussed in subsequent chapter of this book, some Departments of Government of India as well as State Governments had initiated steps to adopt e-Governance. In this context it would be useful to highlight some of the important e-Governance initiatives implemented by the Union and State Governments in the last 10 to 15 years.

3. Overview of National e-Governance Plan (NeGP)

3.1 Emergence of NeGP

राष्ट्रीय इ-गवर्नेंस योजना
National e-Governance Plan
एक कदम आपकी ओर
एक कदम आपके लिए
Public services closer home
www.negp.gov.in

During the 1980s and early 1990s initial attempts towards e-Governance were made basically focusing towards networking government departments and developing in-house government applications in the areas of defence, economic monitoring, planning and the deployment of IT to manage data-intensive functions related to elections, census, tax administration etc. These applications focused on automation of internal government functions rather than on improving service delivery to citizens.

Highlighting this concern, Dr. APJ Abdul Kalam, former President of India and a visionary in the field of e-Governance, in his Inaugural address at IIT Delhi during International Conference on e-Governance, 18th December, 2003 has aptly summarized the basic challenge lying before the country in this regard:

"e-Governance has to be citizen-friendly. Delivery of services to citizens is considered a primary function of the government. In a democratic nation of over one billion people like India, e-Governance should enable seamless access to information and seamless flow of information across the state and central government in the federal set up. No country has so far implemented an e-Governance system for one billion people. It is a big challenge before us."

In recent years, in many forums, the Government of India has indicated their commitment to provide efficient and transparent government to all strata of society. e-Governance is now seen as a key element of the country's governance and administrative reform agenda. The Government of India aspires to provide:

- Governance that is easily understood by and accountable to the citizens, open to democratic involvement and scrutiny (an open and transparent government).
- Citizen-centric governance that will cover all of its services and respect everyone as individuals by providing personalized services.
- An effective government that delivers maximum value for taxpayers' money (quick and efficient services)

Hence the Government of India views e-Governance as a vehicle to initiate and sustain reforms by focusing on three broad areas like Public services, Management and Governance.

The incumbent Union Government's National Common Minimum Program also accords priority to improving the quality of basic governance and in that context proposes to promote e-Governance on a massive scale in areas of concern to the common man.

Experiences from successes as well as the failures of the various initiatives played an important role in shaping the e-Governance strategy of the country. A need was therefore felt for taking a holistic view of several e-Governance initiatives to be implemented across the country. It was increasingly perceived that if e-Governance was to be expedited across the various arms and levels of Government, a program approach would need to be adopted, which must be guided by a common vision, strategy and approach. This approach would have the added advantage of enabling huge savings in cost, in terms of sharing the core and support infrastructure, enable interoperability through standards etc, which would result in the citizen having a seamless view of Government.

The National e-Governance Plan (NeGP) has been formulated by the Department of Information Technology (DIT) and Department of Administrative Reforms & Public Grievances (DAR&PG). The Union Government approved the National e-Governance Plan (NeGP), comprising of 27 Mission Mode Projects (MMPs) and 8 components on May 18, 2006.

The Government has accorded approval to the vision, approach, strategy, key components and implementation framework for the NeGP.

3.2 Vision

NeGP, with the aim of improving delivery of Government services to citizens and businesses, is guided by the following vision:

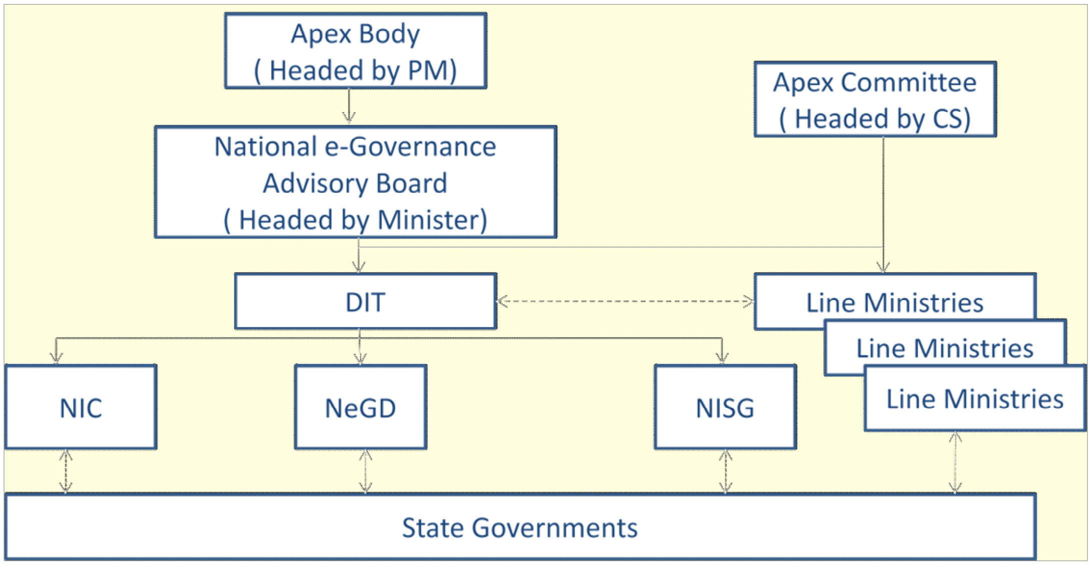
> "Make all Government services **accessible** to the common man in his locality, through **common service delivery outlets** and ensure **efficiency, transparency & reliability** of such services at **affordable** costs to realize the basic needs of the common man."

As can be observed, the vision statement clearly underlines the priorities of the Government in fostering good governance. These are:

- **Accessibility:** The vision has been designed keeping the rural population in mind. The need is to reach those sections of the society which have remained tangential to the government sphere due to various reasons like geographical challenges and lack of awareness. NeGP has a provision for SWAN to connect all the government offices upto the block level and CSCs for accessing the citizens from the rural areas.
- **Common Service Delivery Outlets:** At present citizens, especially those living in remote rural areas have to travel long distances (at times even 100 kms or more) on bumpy roads more than once to avail a service through a government Department or its local office. This process is not just time-consuming and painful but also prohibitively costly for a ordinary citizen, who has to think twice before going to a Government office. To overcome this problem, as a part of the NeGP's Vision, one Common Service Centre (CSC) is envisaged to be opened for every six villages so that easily avail these services and that too with comfort and convenience. These CSCs will offer online **Integrated Service Delivery on 'Anytime, Anywhere' basis.** Moreover, employment opportunities for entrepreneurs would be generated through the establishment of Common Service Centres in rural areas.
- **Adopting e-Governance for improving the Governance:** The use of ICT will enable government to reach citizens thereby improving governance. This will also enable improvement in monitoring and implementing of various government schemes thereby increasing the accountability and transparency in government.
- **Improve the quality of life of citizens**: e-Governance would help in attaining this objective through the provision of citizen centric service delivery thereby providing better turnaround times and convenience in demanding and availing services.
- Hence, the vision is to use e-Governance as the route for governments to strengthen good governance. All services provided through the various e-Government initiatives are expected to assist the governments at the Central and State levels in reaching the yet 'unreached' and enable involvement and empowerment of marginalized groups through their participation in the government processes thereby contributing towards poverty reduction and bridging the sharp social and economic divide.

3.3 Key stakeholders in NeGP

In order to ensure that numerous projects being implemented by the Union and State Government departments are consistent with a broad policy and adhere to common standards, the NeGP established a well defines institutional structure. Since the implementation of e-Governance is a highly complex process and to promote e-Governance on a massive scale requires proper monitoring and control, it becomes essential to have an empowered institutional arrangement to oversee, drive and manage implementation. The arrangements may vary at different levels but there should be consistency of key roles i.e. formulating and ensuring uniform policies and standards, addressing implementation bottlenecks and monitoring progress and desired outcomes. To ensure this at the national level, NeGP has established well-defined institutional structure as depicted below:



The roles and responsibilities of various stakeholders involved in implementation of NeGP are as follows:

- **Apex Body (headed by the Prime Minister):** A body under the chairpersonship of the Prime Minister has been constituted with representation drawn from relevant ministries/ departments, the National Knowledge Commission, the Planning Commission, experts, etc. basically to provide leadership to the NeGP; prescribe deliverables and milestones; and monitor periodically the implementation of NeGP.

- **National e-Governance Advisory Board**, headed by the Minister of Communication & Information Technology has been created, to solicit views of external stakeholders and to provide inputs to the CCEA, advise the government on policy issues and strategic interventions necessary for accelerating introduction of e-Governance across central line ministries and state government departments. The Advisory Group also includes representative from the Planning Commission and 3 to 4 representatives from States/UTs and other line ministries/departments on a rotational basis.

- **Apex Committee (NeGP):** with Cabinet Secretary as its Chairman and Secretary, DIT as its Member Convener has been constituted to oversee the NeGP program and provides policy and strategic directions for its implementation, resolves inter-ministerial issues; moderates and drives services, process Re-engineering and service levels of each MMP, wherever required.

- **Line Ministries/Departments:** are responsible for the implementation of the assigned Mission Mode Projects (MMPs)/Components. Mission Mode Projects are owned and spearheaded by various line ministries for central government, state governments and Integrated projects. The Line ministries/ Departments basically takes ownership of the MMP and conceptualize the project by fixing the objectives, hold consultations with all the stakeholders, prepare comprehensive Project Document including identification of e-services and service levels, obtain sanction for schemes, and implement the project and its various components.

- **State Governments/UT Administrations:** Responsible for implementing State Sector MMPs, under the overall guidance of the respective Line Ministries in cases where central assistance is also required. An Apex Committee at the State level headed by the Chief Secretary is constituted to implement the projects.

- **Department of Information Technology (DIT) including National Informatics Centre (NIC):** DIT serves as a secretariat to the Apex Committee and assists it in managing the NeGP projects. DIT assists National e-Governance Advisory Group and Prime Minister's Office; facilitates implementation of NeGP by various Ministries and State Governments; carries out technical appraisal of all NeGP projects; prepares suitable template(s) for preparing project document(s) (e.g. detailed project report), for use by individual departments; provides technical assistance to various Ministries and State Governments either directly or through NIC or in collaboration with external professional Consultants; undertakes monitoring of all the MMPs.

3.3.1 Other Key Stakeholders

- **Planning Commission and Ministry of Finance:** Allocate funds for NeGP through Plan and Non-plan budgetary provisions and lay down appropriate procedures in this regard.

- **Department of Administrative Reforms & Public Grievances (DAR&PG):** Responsible for generic Process Re-engineering and Change Management, which are desired to be realized across all Government departments. However, concerned Line Ministries / Implementing Agencies are primarily responsible for carrying out the required Process Re-engineering and Change Management; promoting initiatives for Human Resource Development, and training and awareness building.

- **Standardization, Testing, Quality and Certification (STQC) Directorate** has established itself as a premier organization for Quality Assurance in the field of Electronics and Information Technology (IT) in the country. It provides Testing, Calibration, Training and Certification services through its network of test laboratories spread across the country

- **Centre for Development of Advanced Computing (C-DAC)**, is primarily an R & D institution involved in the design, development and deployment of advanced Information Technology (IT) based solutions. CDAC is assisting DIT in in taking major initiatives in this area of e-Governance offering solutions and services.

- **The Controller of Certifying Authorities (CCA)** aims at promoting e-Governance through the wide use of digital signatures

- **National Institute for Smart Government (NISG)** provides consulting and implementation support to both Central and State Government. NISG undertakes diversity of activities viz. preparing e-Governance Road Maps; conceptualizing large IT infrastructure projects; preparing framework, guidelines; developing business models and monitoring & evaluation frameworks, designing architectures and developing standards. Apart from playing a strategic advisory role, NISG also supports central and state governments to improve the delivery of government services, design IT systems to enhance internal efficiencies. A very important task of NISG is to help in nation wide capacity building under NeGP to develop leadership capability and skill-sets within the government for implementing e-Governance Projects. NISG has also helped set up the NeGD for the NeGP.

3.4 Implementation strategy for e-Governance

Implementation of e-Governance is a highly complex process requiring provisioning of hardware and software, networking, process Re-engineering and change management. In the past, it is been observed that number of e-Governance projects have been undertaken through individual initiatives; some of them have succeeded while some have not produced the desired results or withstood the test of time. A prudent approach, therefore, is proposed for the NeGP, which is based on lessons learnt from the past and experiences from successful e-Governance applications that have been implemented nationally and internationally. The approach and methodology adopted for NeGP contains the following elements:

- **Common Support Infrastructure:** NeGP implementation involves setting up of common and support IT infrastructure such as: State Wide Area Networks (SWANs), State Data Centres (SDCs), Common Services Centres (CSCs) and Electronic Service Delivery Gateways.
- **Governance:** Suitable arrangements for monitoring and coordinating the implementation of NeGP under the direction of the competent authorities have been set up. The program also involves evolving/ laying down standards and policy guidelines, providing technical support, undertaking capacity building, R&D, etc. DIT strengthens itself and various institutions like NIC, STQC, CDAC, NISG, etc., to play these roles effectively.
- **Centralized Initiative, Decentralized Implementation:** e-Governance is being promoted through a centralized initiative to the extent necessary to ensure citizen-centric orientation, to realize the objective of inter-operability of various e-Governance applications and to ensure optimal utilization of ICT infrastructure and resources while allowing for a decentralized implementation model. It also aims at identifying successful projects and replicating them with required customization wherever needed.
- **Public-Private Partnerships (PPP) model** is to be adopted wherever feasible to enlarge the resource pool without compromising on the security aspects.
- **Integrative Elements:** Adoption of unique identification codes for citizens, businesses and property is to be promoted to facilitate integration and avoid ambiguity.
- **Program Approach at the National and State levels:** For implementation of the NeGP, various Union Ministries/Departments and State Governments are involved. Considering the multiplicity of agencies involved and the need for overall aggregation and integration at the national level, NeGP is being implemented as a program, with well defined roles and responsibilities of each agency involved. For facilitating this, appropriate program management structures have also been put in place.
- **Facilitating role of DIT:** DIT is the facilitator and catalyst for the implementation of NeGP by various Ministries and State Governments and also provides technical assistance. It serves as a secretariat to the Apex Committee and assists it in managing the program. In addition, DIT is also implementing pilot/ infrastructure/ technical/ special projects and support components. DAR&PG's responsibility is towards Government Process Re-engineering and Change Management, which are desired to be realized across all government departments. Planning Commission and Ministry of Finance allocate funds for NeGP through Plan and Non-plan budgetary provisions and lay down appropriate procedures in this regard.
- **Ownership of Ministries:** Under the NeGP, various MMPs are owned and spearheaded by the concerned line Ministries. In case there are any ongoing projects which fall in the MMP category, they would be suitably enhanced to align them with the objectives of NeGP. For major projects like Bharat Nirman, Rural Employment Guarantee Schemes etc., the line ministries concerned are advised to make use of e-Governance as also automation techniques from the inception stage. States have been given the flexibility to identify a few additional state-specific projects, which are relevant for the economic development of the State.

3.5 Mission Mode Projects (MMPs)

The following is the list of MMPs at central, State and at Integrated level. Some of the MMPs are in advanced stages of implementation, while some are in the conceptualization stage.

No	Projects	Line Ministry / Dept Responsible	Project Brief
Mission Mode Projects - Central Sector			
1.	Passport	Ministry of External Affairs/Ministry of Home Affairs	The Passport Seva Project was launched by the Ministry of External Affairs with the objective of delivering Passport Services to the citizens in a comfortable environment with wider accessibility and reliability.. Various e-services being offered under the MMP include issue / re-issue of Passport, issue of duplicate Passport, issue of Tatkal Passport, change in name, address, ECNR/ ECR suspensions, passport status enquiry etc.
2.	Visa & Immigration	Ministry of External Affairs/Ministry of Home Affairs	In order to Modernize and upgrade the Immigration services, "Immigration, Visa and Foreigners Registration & Tracking (IVFRT)" has been identified and included as one of the MMPs to be undertaken by the Ministry of Home Affairs under the National e-Governance Plan (NeGP). The core objective of this Project is to develop and implement a secure and integrated service delivery framework that facilitates legitimate travelers while strengthening security.
3.	MCA21	Ministry of Corporate Affairs	The projects aims to provide electronic services to the Companies registered under the Companies Act. Various online facilities offered includes allocation and change of name, incorporation, online payment of registration charges, change in address of registered office, viewing of public records and other related services.
4.	Insurance	Department of Banking	MMP aims at facilitating customer services, automating grievance redressal mechanism and, creating a holistic database of insurance users.
5.	Income Tax	Ministry of Finance/Central Board of Direct Taxes	Various important e-services being offered under this MMP includes facility for downloading of various forms, online submission of applications for PAN and TAN, query-based services for allotment of PAN and TAN, e-filing of Income Tax Returns, e-filing of TDS returns, online payment of Taxes, issue of refunds through Electronic Clearance Scheme (ECS) and Refund Banker, etc
6.	National Citizen Database/UID	Ministry of Home Affairs/Registrar General of India (RGI)/ Planning Commission	This MMP aims towards creating a Central database of resident information and assign a Unique Identification number to each such resident in the country, to facilitate efficient delivery of social and welfare services.

No	Projects	Line Ministry / Dept Responsible	Project Brief
7.	Central Excise	Department of Revenue/Central Board of Excise & Customs	This MMP aims towards facilitating availability of e-services related to indirect taxation for industry, importers and exporters, inbound travellers etc. Various important e-services being offered include e-filing of Import and Export documentation, electronic processing of declarations, facilities for e-filing of Central Excise and Service Tax returns, e-registration services, digital signatures, e-payment of Customs Duties etc.
8.	Pensions	Department of Pensions & Pensioners Welfare and Department of Expenditure	This MMP provides updated information on government pension rules and regulations; helps facilitating registration of pensioners' grievances; enables monitoring timely sanction of pension/gratuity; maintains a database of Pensioners and providing links to the websites of the Directorates of Pensions and the AGs of various States.
9.	Banking	Department of Banking	This MMP aims towards streamlining various e-services initiatives undertaken by individual banks.
10.	e-Office	Department of Administrative Reforms & Public Grievances	This MMP aims at significantly improving the operational efficiency of the Government by transitioning to a "Less Paper Office".
Mission Mode Projects - State Sector			
1.	Land Records	Ministry of Rural Development	The project - National Land Records Modernization Program (NLRMP) aims towards providing integrated land related information and services to citizens. Various online services provided are issue of copies of RORs, crop; irrigation details, filing and tracking of mutation cases, availability and submission of forms
2.	Road Transport	Ministry of Road Transport & Highways	The project aims to induct technology in transport offices across India to offer vehicle registration, driving licenses and Smart Card based RCs (Registration Certificates) to citizens.
3.	Agriculture	Department of Agriculture & Cooperation	The MMP aims at providing information regarding farm practices, market trends, agricultural and technical know-how, providing online certification / licenses to wholesalers and retails dealing in pesticides, fertilizers etc. and other related services to the farming community.

No	Projects	Line Ministry / Dept Responsible	Project Brief
4.	Treasuries	Ministry of Finance	This MMP aims at computerisation of treasuries involving common set of standards for seamless integration of participating agencies.
5.	Municipalities	Ministry of Urban Employment and Poverty Alleviation	The MMP aims at providing various services offered by Urban Local Bodies (ULBs) to residents electronically.
6.	Gram Panchayats	Ministry of Panchayati Raj	The MMP aims at improving governance at the grass roots and providing various e-services at the Panchayat level.
7.	Commercial Taxes	Ministry of Finance	The MMP, which aims at providing electronic services to commercial taxes payers, is being formulated.
8.	Police (CCTNS)	Ministry of Home Affairs	The Mission Mode Project of the Police - Crime and Criminal Tracking Network System (CCTNS) - - is aimed at facilitating the process of civil policing and law enforcement by utilizing ICT effectively. Among many other services, it will allow citizens to register and track an online complaint
9.	Employment Exchanges	Ministry of Labour & Employment	This MMP of the Ministry of Labour aims at providing e-services to employment seekers and employers.
10.	E District	Department of Information Technology	The MMP aims at delivery of high volume, citizen-centric services at the District level such as issue of birth/death certificate, income and caste certificate, old age and widow pension etc.
Mission Mode Projects - Integrated Category			
1.	EDI (e-Commerce)	Ministry of Commerce & Industry/ Department of Commerce	The MMP aims at facilitating Electronic Data Interchange amongst various agencies involved in the process of Imports and Exports.
2.	e-Biz	Department of Industrial Policy & Promotion / Department of Information Technology	The project aims to provide comprehensive Government-to-Business (G2B) services to business entities with transparency, speed, and certainty
3.	Common Services Centres	Department of Information Technology	The MMP is a part of the core and support infrastructure of NeGP and aims towards offering e-Governance services to rural citizens.

No	Projects	Line Ministry / Dept Responsible	Project Brief
4.	India Portal	Department of Information Technology and Department of Administrative Reforms & Public Grievances	The MMP aims towards providing a single window access to information and services of Government at all levels, in a multilingual form.
5.	National Service Delivery Gateway (NSDG)	Department of Information Technology	The MMP aims at providing a common interface between the service seekers and service providers (Government Department).
6.	e-Courts	Department of Justice, Ministry of Home Affairs	The MMP aims at utilizing technology for improved provisioning of judicial services to citizens.
7.	e-Procurement	Ministry of Commerce & Industry/ DGS&D	The MMP of the Ministry of Commerce aims at rolling-out IT-enabled procurement by Government Departments.

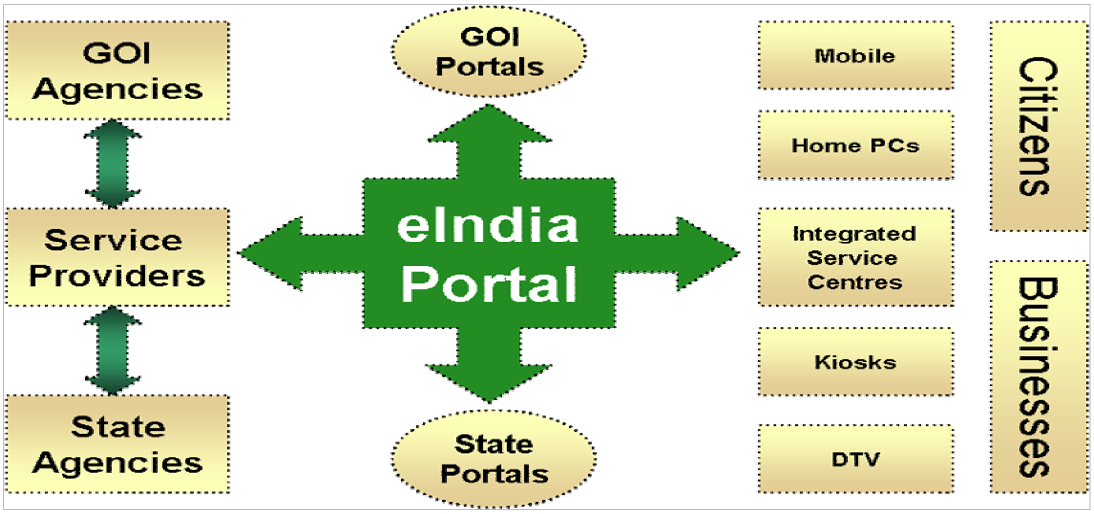
3.6 Components of NeGP

For the implementation of NeGP, DIT is creating Common Core and Support Infrastructure (National/State Wide Area Networks, National/State Data Centres, CSCs & Electronic Service Delivery Gateways) and has made suitable arrangements for monitoring and coordinating the implementation of NeGP under the directions of the competent authorities in this regard. The 8 key components identified for successful implementation of various e-Governance Projects is as below:

Sr. No	Support Components	Line Ministry / Department Responsible
1.	Core Policies	DIT
2.	Core Infrastructure (SWAN, NICNET, SDCs, etc.)	DIT
3.	Support Infrastructure (CSCs, etc.)	DIT
4.	Technical Assistance	DIT
5.	R&D	DIT
6.	Human Resource Development & Training	DIT and DAR&PG
7.	Awareness & Assessment	DIT and DAR&PG
8.	Organization structures	DIT and DAR&PG

3.7 NeGP Framework

The e-Governance framework would include Back-ends (databases of the different government agencies, service providers, state governments etc.), Middleware and the Front-end delivery channels (home PCs, mobile phones, kiosks, integrated citizen service Centres etc.) for citizens and businesses. The Middleware comprises of communication and security infrastructure, gateways and integrated services facilitating integration of inter-departmental services. The following figure provides the depiction of the NeGP framework:

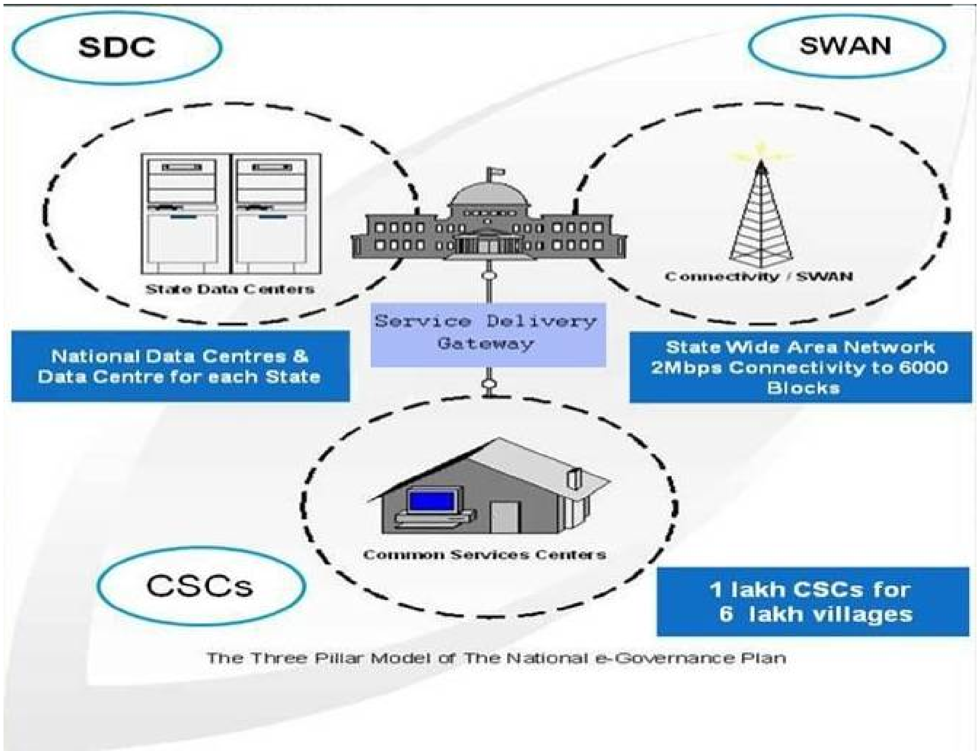


NeGP Program Framework

3.8 Core and support infrastructure of NeGP

Under NeGP, all services are supported by three infrastructure pillars for efficient delivery of "web-enabled" anytime anywhere access to information and service across the country, NeGP envisions 3 pillars of e-Governance infrastructure namely:

a) State Wide Area Network (SWAN)
b) National Data Bank/State Data Centres (SDC)
c) Common services Centres (CSC)


SDC
SWAN
State Data Centers
Service Delivery Gateway
Connectivity / SWAN
National Data Centres & Data Centre for each State
State Wide Area Network 2Mbps Connectivity to 6000 Blocks
Common Services Centers
CSCs
1 lakh CSCs for 6 lakh villages

The Three Pillar Model of The National e-Governance Plan

a) State Wide Area Networks (SWANs)

State Wide Area Network (SWAN/NICNET) which will provide connectivity at 2 mbps up to the block level. It is also envisaged that SWANs will have base stations to enable wireless connectivity beyond block level.

The Government approved the Scheme for establishing State Wide Area Networks (SWANs) across the country. The objective of the Scheme is to create a secure close user group (CUG) government network for the purpose of delivering G2G and G2C services. The duration of project is 5 years with a pre-project implementation period of 18 months. The project is being implemented as a Central Sector Scheme with Rs.2005 Crores as Grant-in-aid from Department of Information Technology and balance fund from the State Plan fund under Additional Central Assistance (ACA) allocation.

The salient features of the SWAN scheme as envisaged under the NEGP are:

- One PoP at each State/ District/ Block Headquarter
- Bandwidth capacity (at least 2 Mbps for each link)
- Appropriate Service Level Agreement tied up with Bandwidth Service Provider/ Network Operator
- PoPs designed as configurable Bandwidth Aggregation points with scalability to enable vertical & horizontal connectivity
- Gateway to NICNET at State/UT headquarter PoP for Central Services
- Connectivity to Data Centre and Disaster Recovery Centre
- Network Performance Audit

The SWAN Scheme for 29 States & 6 Union Territories, at an estimated outlay of Rs. 3334 Crore, was approved by Government of India, in March 2005 to set up State Wide Area Networks (SWAN), interconnecting each State / UT Head Quarter with District Head Quarter and below each District Head Quarter with the Block Head Quarters with minimum 2 Mbps leased line.

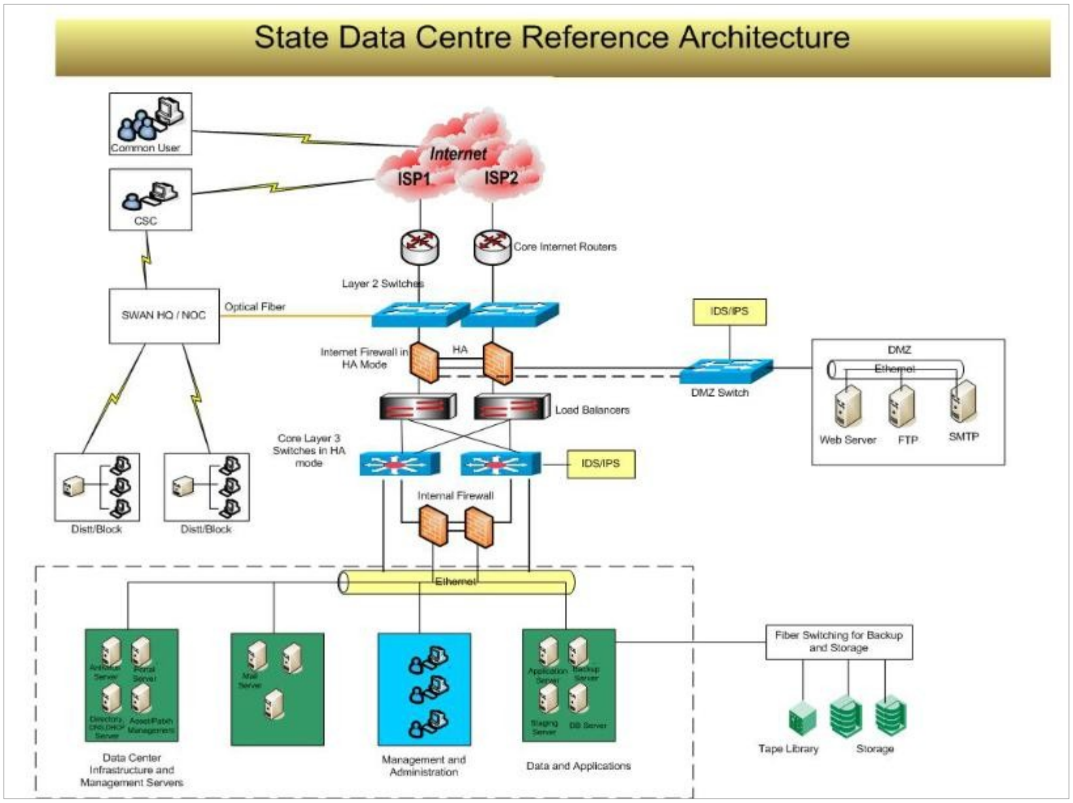
SWANs across the country, when fully implemented, will create more than one million route - km of network connecting more than 100,000 government entities. This would bring a connected government space which is unprecedented and would bring a paradigm shift in the way the government works for itself and for the citizen. Success of various e-Governance initiatives taken up at the State and the Central level would heavily depend on maximum utilization of SWANs.

b) State Data Centre (SDC)

State Data Centre (SDC) has been identified as one of the important elements of the core infrastructure for supporting e-Governance initiatives of National e-Governance Plan (NeGP).

The concept of the State Data Centres is designing of State Data Centres for the States to consolidate infrastructure, services and application to provide efficient electronic delivery of G2G, G2C and G2B services. These services can be rendered by the States through common delivery platform seamlessly supported by core Connectivity Infrastructure such as State Wide Area Network (SWAN) and Common Services Centre (CSC) at the village level.

State Data Centre would provide many functionalities and some of the key functionalities are Central Repository of the state, Secure Data Storage, Online Delivery of Services, Citizen Information/Services Portal, State Intranet Portal, Disaster Recovery, Remote Management and Service Integration etc. SDCs would also provide better operation & management control and minimize overall cost of Data Management, IT Resource Management, Deployment and other costs. The following is the bundle of services expected to be provided by the SDC.



The objectives for design of SDC are:

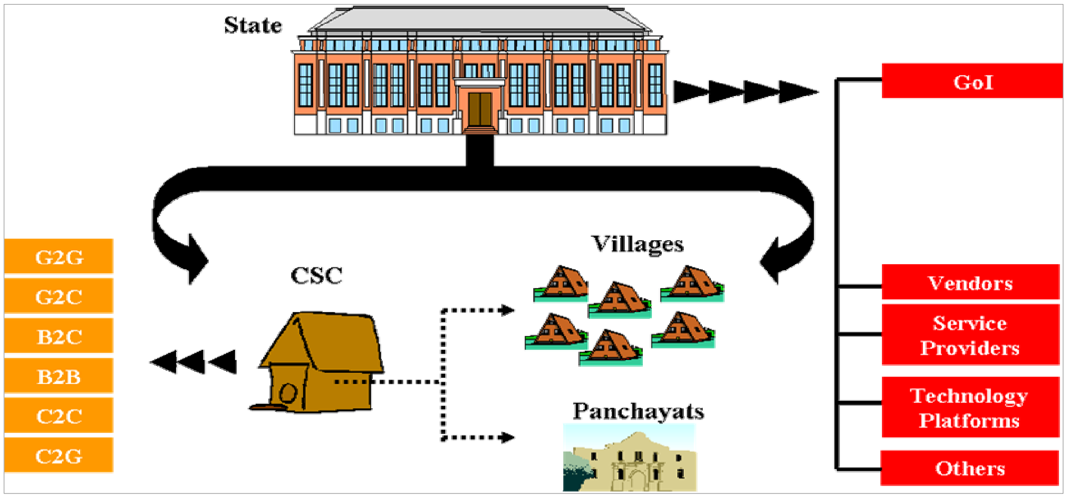
- Availability of 'IT Infrastructure' to State Departments and Agencies
- Enhanced reliability
- Higher availability of system and data - 99.74%

- Guaranteed Service Levels
- Efficient & effective management of Information Security related issues
- Centralized and Simplified Management
- Improved quality of Data housekeeping
- Dynamic Scalability
- Lower risk of data loss
- Better management of security & access control
- Faster Implementation cycle

Department of Information Technology (DIT) has formulated the guidelines to provide Technical and Financial assistance to the States for setting up State Data Centres. These guidelines also include the implementation options that can be exercised by the state to establish the SDC. SDC scheme has been approved by the government with an outlay of Rs.1623.20 crores over a period of 5 years.

c) Common Service Centres (CSCs)

The Government has approved a Common Services Centres (CSCs) Scheme for providing support for establishing 100,000 Common Services Centres in 600,000 villages of India. The scheme, as approved by the Government of India, envisions CSCs as the front-end delivery points for government, private and social sector services to rural citizens of India, in an integrated manner. The objective is to develop a platform that can enable government, private and social sector organizations to align their social and commercial goals for the benefit of the rural population in the remotest corners of the country through a combination of IT-based as well as non-IT-based services.



CSC Ecosystem

The Scheme has been approved at a total cost of Rs. 5742 Crores over 4 years, of which the Government of India is estimated to contribute Rs. 856 Crores and the State Governments Rs.793 Crores. The balance resources would be mobilized from the private sector. The Common Services Centres would be designed as ICT-enabled Kiosks having a PC along with basic support equipment like Printer, Scanner, UPS, with Wireless Connectivity as the backbone and additional equipment for edutainment, telemedicine, projection systems, etc., as the case may be.

The Scheme is to be implemented through a Public Private Partnership. CSCs are the primary physical front-end for delivery of Government and private services to citizens. They are one of the three pillars of the core and support infrastructure of the National e-Governance Plan for enabling anytime anywhere delivery of government services, the other two being (a) the State Wide Area Network (for Connectivity) which has already been approved by the Government for Rs.3334 Crores and (b) the State Data Centre Scheme (for secure hosting of data and applications) for which the draft guidelines are under preparation.

The Scheme is being implemented through a Public Private Partnership. CSCs are the primary physical front-end for delivery of government and private services to citizens. They are one of the three pillars of the core and support infrastructure of the National e-Governance Plan for enabling anytime anywhere delivery of government services, the other two being (a) the State Wide Area Network (for Connectivity) which has already been approved by the Government for Rs.3334 Crores and b) the State Data Centre Scheme (for secure hosting of data and applications) for which the draft guidelines are under preparation.

Implementation of a mission-oriented project of this size and scope would pose significant challenges of project management at the national level as also in exploiting opportunities to achieve significant economies of scale in the identification, customization and implementation of the physical and digital infrastructure required for the project. Further, many of the potential citizen-centric services would lend themselves to aggregation at the national level. To serve the above objectives and to enable the state-specific implementation plans to benefit from such economies of scale, aggregation of best practices, content providers, etc. DIT has appointed a National Level Service Agency (NLSA) with defined Terms of Reference to coordinate the entire activity. The CSC Scheme has a 3-tier implementation framework:

- At the first (CSC) level would be the local Village Level Entrepreneur (VLE- loosely analogous to a franchisee), to service the rural consumer in a cluster of 5-6 villages.
- At the second/middle level would be an entity termed the Service Centre Agency (SCA loosely analogous to a franchiser) to operate, manage and build the VLE network and business. An SCA would be identified for one or more districts (one district would cover 100-200 CSCs).
- At the third level would be the agency designated by the State- the State Designated Agency (SDA) - to facilitate implementation of the Scheme within the State and to provide requisite policy, content and other support to the SCAs.

d) State e-Governance Service Delivery Gateway (SSDG)

SSDG is a middleware that is being positioned in all the States/ UTs and also at the national level (www.nsdg.gov.in) as a soft-infrastructure piece for the delivery of e-Governance services. The purpose of this middleware is to de-couple the front-end and the back-end in the delivery of services to ensure scalability, inter-operability between heterogeneous systems, authentication, ensure assured delivery, message routing, transaction logs, audit trails, time-stamping etc. and in future also provide for joined-up and integrated services. This middleware has a larger scope than being used in a single project and will lead to convergence of the proposed model with the other MMPs (like e-District) as and when they are realized. SSDG will be hosted in the State Data Center (SDC).

The objectives of the NSDG / SSDG are:

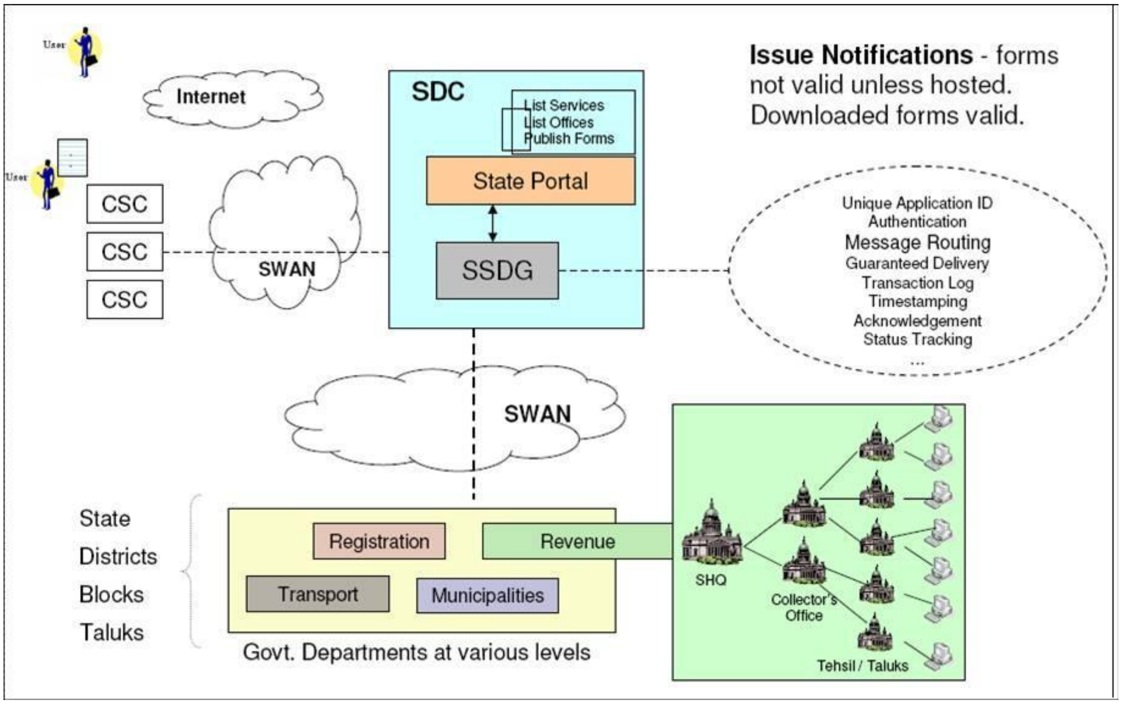
- Act as a catalyst in enabling the building of standards based e-Governance applications with Gateway as the middleware to ensure interoperability
- Enable integration across Centre, State or Local Governments there by enabling Integrated
- Service Delivery and a Service Oriented Architecture (SOA) leading to joined up government
- Help protect the legacy investments in software and hardware by easily integrating them with other technology platforms and software implementations
- De-link the back-end departments/Service Providers (SP) from the front-end Service Access
- Providers thereby
    - Ensuring separation of concerns of service access from the service implementation i.e. separates the Portal, CSC, Kiosks etc. from the government services which reside in the back-end departments.
    - Encouraging competition at the front-end by allowing independent service access providers to provide services with varying levels of complexity, cost and service quality levels.

- Shared services can be added on to the core services as and when required, as special common services of the Gateway without affecting the core functionality of the Gateway, thereby providing flexibility and modularity.
    - o encourage back-end services to be plugged into the infrastructure as and when they are ready,
- Reduce the cost of e-Governance Projects by rationalizing, distributing and optimizing the services framework
- Use PKI infrastructure for secure transactions. Provision exists for encryption of department payload to ensure confidentiality of department data. The gateway provides digital signature and certificates to all stakeholders interacting with the gateway for identification, authentication and authorization. Transaction and audit logs help track government data.
- Enable transaction logging and time stamping for tracking of transactions and centralized control
- Help the Departments backend workflow evolve gradually as the Gateway acts as a middleware de-linking the back-end from the front-end. This means that even the Departments which do not have the complete automation or work flow at the back can still deliver e-Service to the citizens in a limited manner through the Gateway. To cite as an example, a server may be put up at the department for message exchange with Gateway in absence of readily available infrastructure at the department.

NSDG I SSDG Conceptual Architecture and Gateway Messaging specifications

SSDG as a messaging middleware acts as an intelligent hub and routes service requests from a Service Seeker (Service Access Provider) to a Service Provider (typically a back-end Government department that puts up its service for electronic delivery) and in return sends the response back to the Service Seeker through the Gateway.

The following figure illustrates the SSDG structure linking up the Service Seekers (citizens and businesses), Service Access Providers and the Service Providers (government departments or third party service providers).



The SSDG will link two major entities:

1. Service Providers (SP): The back-end government departments or any other third-party agencies offering e-Services to citizens and businesses, and to other government departments, are collectively referred to as Service Providers (SP). Third-party SPs may offer specialized services such as authentication, payment gateway services, or joined-up services.

2. Service Access Providers (SAP): A Service Access Provider is an entity, which facilitates government service access by Service Seekers, by providing a front-end infrastructure. 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.

4. e-Governance Project Development Lifecycle

This section discusses the Lifecycle of an e-Governance project including various phases in the Lifecycle, activities performed in each phase along with the outputs at each phase.

4.1 Challenges in current environment (e-Governance Projects)

Following discusses the key challenges in various e-Governance projects implemented at Central / State / local government level.

Identify
Assess
Plan
Implement
Communicate

- Many of the projects are towards computerization, but not modernization (reason: As-Is computerization)
- Significant investments into projects with minimal impact/improvement in service delivery and administration
- Minimal online or self services to the stakeholders
- IT enabled processes with no improvement in the service levels
- Projects not completed in time - delayed for years
- IT systems not meeting the business requirements - common challenge
- Low return on investment (value in terms of reduction in service delivery timelines, administrative burden, improvement in SLA's, quality of service)
- Failure in meeting defined project objectives (if any are defined)
- Poor quality of the product & services (performance of product and vendor)
- Vendor lock-in
- And many more

4.2 Some key factors contributing to current environment

Following lists some key factors contributing the key challenges listed above.

- Project design incompatible with current readiness and environment
- Least time spent by the organizations in planning and design
- Lack of clear and measurable project goals, objectives and anticipated benefits
- Larger emphasis on IT enablement with minimal focus on business benefits
- Minimal focus on key project enablers (GPR, people change, capacity building..)
- Minimal focus on project and systems quality assurance
- Poor communication to the stakeholders and users on objectives and benefits
- Inadequate resources for project (people and funding)
- Lack of capacities to conceptualize and manage e-Governance projects
- Senior leadership attention towards e-Governance initiatives is minimal - often regarded as a low priority
- Lack of stable project and permanent leadership with managerial powers to drive projects
- Lack of capacities to conceptualize and manage e-Governance projects
- Minimal focus on key project enablers (GPR, people change, capacity building..)
- Poor communication to the stakeholders and users on objectives and benefits

- Inadequate resources for project (people and funding)
- Minimal focus on project and systems quality assurance

4.3 Need for a more robust approach for e-Governance

For addressing the above discussed challenges, it requires a comprehensive and robust approach for conceptualization, implementation and maintenance of an e-Governance project. The approach shall support government or public sector organizations to:

- Get it right first time
- Orient project designs with customer focus and needs
- Achieve heightened focus on business and stakeholder benefits
- Prioritization of requirements in line with business and stakeholder needs
- Support in adoption of best practices and right approach at each phase
- Manage the private sector participation and project delivery to the results
- Phased implementation with minimal impact and maximum results to stakeholders

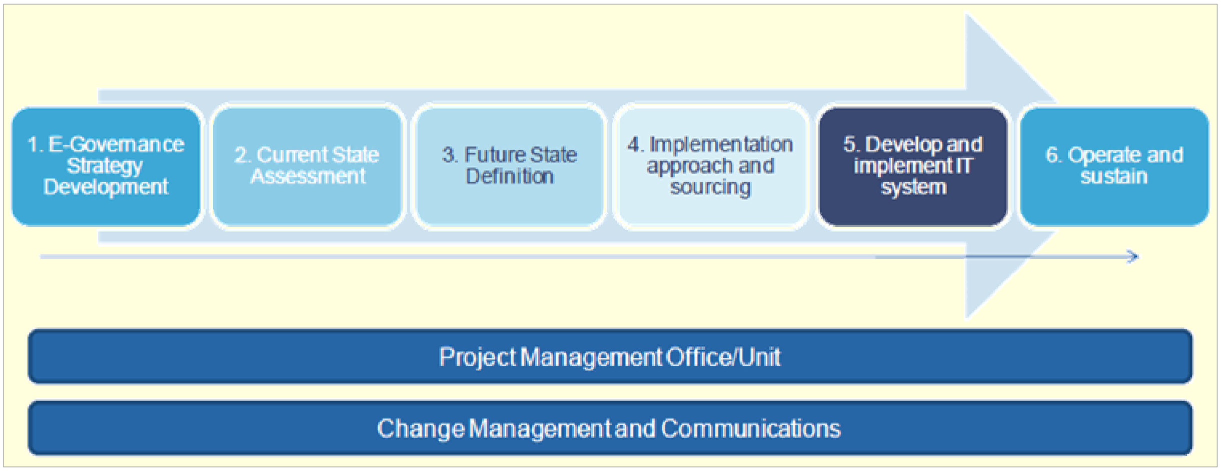
4.4 Essential elements of e-Governance project

Following lists some key and essential elements of an e-Governance project.

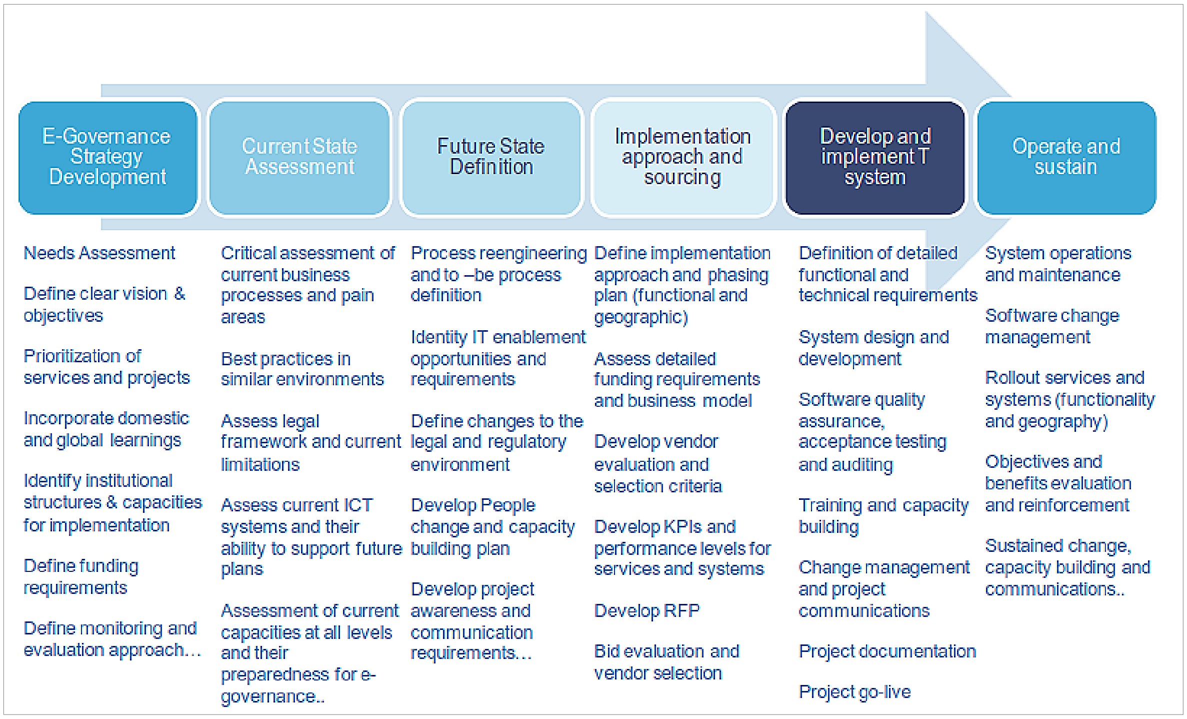
- Vision and strategy
- Business Process Re-engineering
- Enterprise Architecture
- Software development and IT Infrastructure implementation
- Business model
- Legal Framework
- Change Management
- Training and Capacity Building
- Project and Program Management
- Monitoring & Evaluation

4.5 e-Governance Project Lifecycle

The diagram below presents an overview of Lifecycle of an e-Governance project followed by a list of key activities performed at phase of the Lifecycle.


1. E-Governance Strategy Development
2. Current State Assessment
3. Future State Definition
4. Implementation approach and sourcing
5. Develop and implement IT system
6. Operate and sustain
Project Management Office/Unit
Change Management and Communications

The diagram below lists the key activities performed at various phases of e-Governance project Lifecycle.



E-Governance Strategy Development	Current State Assessment	Future State Definition	Implementation approach and sourcing	Develop and implement T system	Operate and sustain
Needs Assessment Define clear vision & objectives Prioritization of services and projects Incorporate domestic and global learnings Identify institutional structures & capacities for implementation Define funding requirements Define monitoring and evaluation approach…	Critical assessment of current business processes and pain areas Best practices in similar environments Assess legal framework and current limitations Assess current ICT systems and their ability to support future plans Assessment of current capacities at all levels and their preparedness for e-governance..	Process reengineering and to –be process definition Identity IT enablement opportunities and requirements Define changes to the legal and regulatory environment Develop People change and capacity building plan Develop project awareness and communication requirements…	Define implementation approach and phasing plan (functional and geographic) Assess detailed funding requirements and business model Develop vendor evaluation and selection criteria Develop KPIs and performance levels for services and systems Develop RFP Bid evaluation and vendor selection	Definition of detailed functional and technical requirements System design and development Software quality assurance, acceptance testing and auditing Training and capacity building Change management and project communications Project documentation Project go-live	System operations and maintenance Software change management Rollout services and systems (functionality and geography) Objectives and benefits evaluation and reinforcement Sustained change, capacity building and communications..

4.5.1 eGLC vs Software Development Lifecycle (SDLC)

The table below compares Software Development Lifecycle and e-Governance Lifecycle.

SDLC	eGLC
• Focuses activities performed at each stage of a software development • Methodology used from the conception phase through to the delivery • Focuses on technical artifacts and right approach for software design, development, implementation and management • Focuses on technical and process related aspects of software • Focuses Software Quality Assurance to get the end product in line with defined requirements	• SDLC is an integral part and only a component of eGLC • eGLC focuses on business and stakeholder needs and priorities • Outcomes and benefits oriented approach • All-encompassing with focus on other critical enablers (GPR, people, legal, M & E)

4.5.2 e-Governance Project Lifecycle

(a) Phase 1: e-Governance Strategy Development

The table below lists key activities performed in e-Governance Strategy Development phase and illustrative deliverables.

Key Activities	Deliverables

• Needs Assessment • Define clear vision & objectives • Prioritization of services and projects • Incorporate domestic and global learning • Identify institutional structures & capacities for implementation • Define funding requirements • Define monitoring and evaluation approach	• e-Governance vision • e-Governance Objectives • e-Governance Strategy

(b) Phase 2: Current State Assessment

The table below lists key activities performed in Current State Assessment phase and illustrative deliverables.

Key Activities	Deliverables
To perform an in-depth assessment of business functions and services identified for coverage under e-Governance project to understand: • Current approach for performing the business functions and service delivery • The key challenges and to identify improvement areas • Stakeholder needs and expectations • Good practices and learning from similar implementations in similar domains • Current systems (IT) implemented in the department, coverage and gaps • Organization structures and people capacities etc	• Process maps • Pain points • Initial improvement areas • Stakeholder needs • IT Systems • Scope and functionality • Strengths and gaps • IT Infrastructure (network, security, data center) • Organizational structures • Roles and responsibilities • Capacities and skill sets • Change barriers

(c) Phase 3: Define Future State (To-be definition)

The table below lists key activities performed in Future State Assessment phase and illustrative deliverables.

Key Activities	Deliverables
• To define how the identified business functions and services shall be performed going forward • To define the new business processes • To define IT solutions and services for automation of new business processes • To define people change management, capacity building and communication requirements for project implementation	• To-be business processes • New process KPIs/metrics • Changes to the legal and policy environment • Functional Architecture and Requirements specifications • Enterprise Architecture covering Application, data, network, security, data center architecture • Data digitization and migration strategy • SLAs • Institutional structures needed for project implementation • Training and Capacity building plan • Change Management Plan • Communications Management Plan

(d) Phase 4: Implementation approach and sourcing

Key Activities	Deliverables
• Development of Implementation Approach and Plan • Development of Business Model • RFP Development • Vendor Evaluation and Selection	• Implementation Approach and Plan • Implementation timelines • Identification of key stakeholders and their roles and responsibilities • Monitoring and Evaluation (M & E) Plan • Project investments and costs • Business/implementation model • Payment terms • SLAs • Procurement approach • Request for Proposals (RFP) • Contract Documents/Agreements • Pre-bid minutes and clarifications • Vendor evaluation reports • Vendor (s) identification • Signed contract documents

(e) Phase 5: Develop and Implement IT System

Key Activities	Deliverables
• Application Software Development • IT Infrastructure Creation • Third Party Acceptance Testing • Training and Capacity Building	• e-Governance Solution/Software • IT Infrastructure

(f) Phase 6: Operate and Sustain

Key Activities
• IT Systems Operations and Maintenance • Monitoring and Evaluation

4.5.3 Project Management Office/Unit

Key Activities

- Definition of Program and Project implementation plans
- Identification of stakeholders and key responsibilities
- Identification of external support needed from market (consultancy services, software development, IT infra creation, change management)
- Definition of scope of work for the vendors
- RFP Preparation and vendor selection
- Monitoring project implementation plans
- Scope change management
- Risk assessment and management
- Issue Management
- Services/Systems quality assurance
- SLA Monitoring
- Project financial management
- Change Management and Communications
- Training and Capacity building
- Monitoring and Evaluation of project objectives and benefits

4.5.4 Change Management and Communications

Key Activities

Change Management

- Understand the changes lead by the project (policy, processes, systems)
- Identify the impacted stakeholders
- Assess the readiness of stakeholders to adopt change
- Identity key risks surrounding resistance to change
- Devise measures to address the identified risks
- Develop change management strategy
- Implement strategy
- Monitoring and corrective actions

Project Communications

- Understand the project scope and coverage
- Identify the objectives, benefits
- Identify the stakeholder groups impacted by the project
- Identify the communication needs for each stakeholder group
- Identify the communication channels
- Development communications management strategy
- Implement strategy
- Monitoring and corrective actions

Capacity Building

- Understand the changes lead by the project (policy, processes, systems..)
- Identify the impacted stakeholders
- Understand the skill sets needed to adopt the new systems and processes
- Assess the current skill sets and capacities in the organization
- Identify the training needs to bridge the gaps in the skill set.
- Identify the training courses and approach for training
- Implement Training Plan

5. Success stories

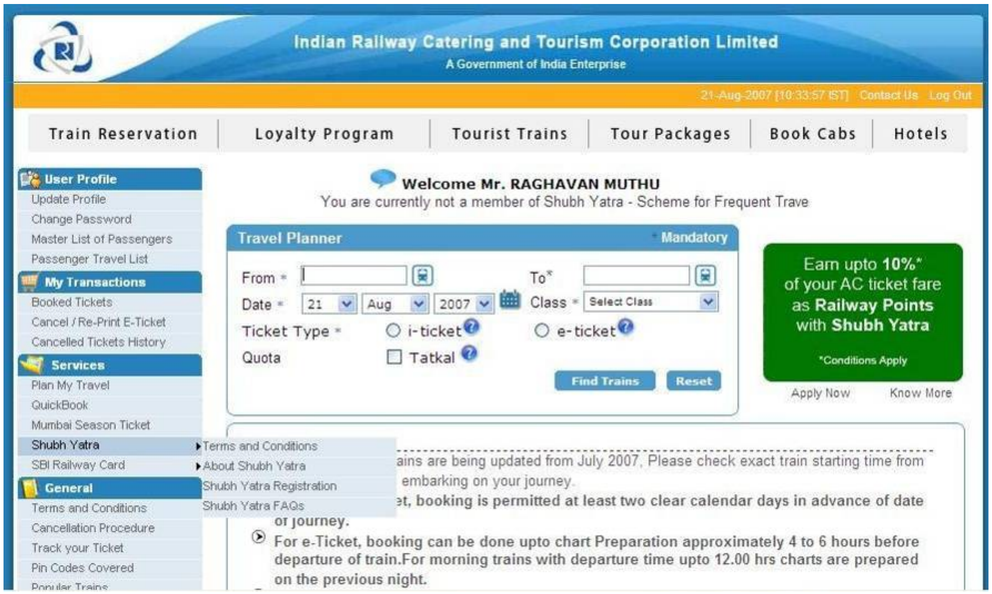
e-Governance has gone beyond the computerization of government processes and into the realms of good governance leading to vast opportunities for transforming governance. Hence, e-Governance in India has provided an important platform to upscale and integrate various e-Governance initiatives at district, state and individual Ministry level.

The recent Nation-wide Impact Assessment exercise undertaken by the Department of Information Technology (DIT) on the three National level projects (MCA21, Passport, Income Tax) and three State level projects (Land records, Property Registration, Transport) endeavors to provide insightful and comprehensive analysis of how far e-Governance have been able to provide electronically enabled services to the common man.

5.1 e-Governance Success Stories - Central Sector MMPs

Some of the projects that have become success stories at the central government level and that have significantly impacted the day to day life of the common citizen are:

5.1.1 Indian Railways Reservation System



Indian Railway Catering and Tourism Corporation Limited
A Government of India Enterprise

21-Aug-2007 [10:33:57 IST]

Welcome Mr. RAGHAVAN MUTHU
You are currently not a member of Shubh Yatra - Scheme for Frequent Trave

Travel Planner
* Mandatory

From *
To*
Date * 21 Aug 2007
Class * Select Class
Ticket Type * ○ i-ticket ○ e-ticket
Quota □ Tatkal

Earn upto 10%* of your AC ticket fare as Railway Points with Shubh Yatra
*Conditions Apply

ains are being updated from July 2007. Please check exact train starting time from embarking on your journey.

ɜt, booking is permitted at least two clear calendar days in advance of date of journey.

For e-Ticket, booking can be done upto chart Preparation approximately 4 to 6 hours before departure of train.For morning trains with departure time upto 12.00 hrs charts are prepared on the previous night.

Till early 90s the train reservation system was manual. The issues were as follows:

- A normal citizen was expected to come to a particular counter to book a reservation
- Return reservation was a big challenge
- The confirmation of the seat was not possible instantly
- Speed money was very common to get a reservation due to non-transparency

However post the reservation, it was possible to do the business process Re-engineering aimed at citizen convenience. Today the citizen has significant convenience as compared to 20 years back, viz:

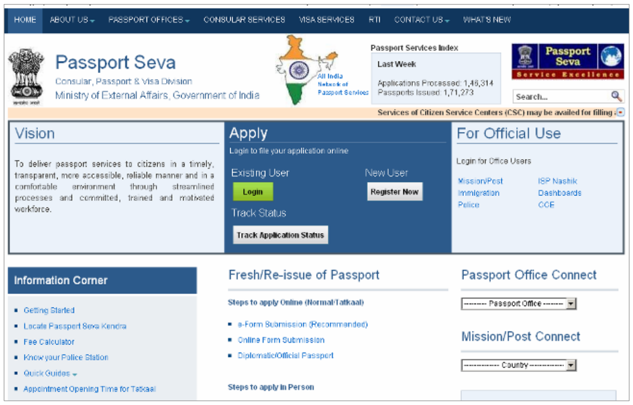
- Passengers can book any train from any booking location
- Information regarding the availability of seats is easily available
- Reservations can be made through website - a transparent system
- Railway Call Centre supported by Interactive Voice response System

5.1.2 Passport

Key challenges:

1. Queue Management system:

- Time taken for submission of the application was more than 2 hrs
- Unclear guidelines and lack of awareness among applicants
- Less number of counters for accepting applications
- Seating arrangements not based on the number of transactions
- Space constraints in the offices



Passport Services Index

Last Week

Applications Processed: 1,46,314
Passports Issued: 1,71,273

Services of Citizen Service Centers (CSC) may be availed for filling

To deliver passport services to citizens in a timely, transparent, more accessible, reliable manner and in a comfortable environment through streamlined processes and commited, trained and motivated workforce.

Login to file your application online

Login for Office Users

Steps to apply Online (Normal/Tatkaal)

Steps to apply in Person

2. Infrastructure and public utilities: “Need for overall improvement in the public utilities such as Water, Canteen, Toilets, Seating arrangements etc.”

3. Variations in service levels: Different service levels for processing applications

4. Delay due to Police Verification Process: "Manual procedures for sending the applications for police verification leading to delay in the overall procedure"

Pain areas (Based on actual survey done on Passport applicants):

- Many citizens complained that the online tracking system was incorrect
- Only 7% of the respondents received their passport within the stipulated time of 35 days
- 63% were willing to pay more for submission through an online system
- 44% felt that the queue management system was not effective
- 46% of respondents felt that the staff was efficient & supportive, and 43% of the respondents felt otherwise
- 47% disagreed that there was proper public infrastructure available

A BPR exercise was carried out and the revised processes which were the outcome of this exercise are mentioned below:

a) Outsourcing of the front-end activities (Facilitation Centres) of the passport issuance system

- No citizen needs to visit the back-office (i.e. the RPOs)
- Outsourcing for application submission, data entry, receipt of fees, verification of original documents, enquiry and grievance acceptance

b) "Anywhere Anytime Application submission and real-time Status Tracking"

- Online submission, 24x7 through any internet facility (Internet Kiosk, Home)
- Real-time tracking through centralized system

c) Assess the possibility of increasing the number of Government officials who could verify the documents

- Officials issuing verification certificates for passport related services

d) Linkage of the Passport office with a designated point at the police department

- Auto-segregation of application details for police verification (Adverse and clear flagged separately)

- Automated update of the PV status- leading to reduction in overall processing
- Automated reminder for clearance of pending reports

e) Centralized back-office

- Centralized printing of the passports for the Missions/Passport offices to control pendency
- High quality fast printers for centralized back-office
- Printing of e-Passports (Diplomats)
- Outsourcing of the centralized back-office

f) Exception handling for review I objection cases

- Automatic escalation of the objection cases by the system
- Objection cases-Police Adverse cases, PAC Check etc.

5.1.3 Ministry of Corporate Affairs (MCA)

MCA 21 is an innovative e-Governance initiative that aims at continuously repositioning the Ministry of Company Affairs (MCA) as an organization capable of fulfilling the aspirations of its stakeholders in the 21st century. This program builds on government's vision to introduce a service oriented approach in design and delivery of government services, establish a healthy business ecosystem and make the country globally competitive.

The program will provide customers easy and secure access to MCA services, through the infrastructure being setup for the purpose, any time and from any place and in a manner that best suit the stakeholders. The focus of the program is to bring about a fine balance of the stakeholder requirements - between facilitation and control - as a blend of well-defined goals and performance metrics. Adopting international best practices, the goals have been set to bring immense value to the stakeholders.

This project is conceived with visionary goals and objectives for which, NISG had prepared a RFP based on which the implementation partner has been selected in November 2004. A consortium led by TCS with CMC as partner has been awarded the responsibility of implementing the project on a PPP model and the solution deployment started in March 2005. The project has gone live on March 16, 2006, with the launch of the project by the honorable prime minister. The key findings of the study across projects show that:

- The number of trips to Governments offices have reduced from 8 trips to 1-2 trips.
- Waiting time at the offices has reduced in the range 20-40%.
- People show strong preference to computerized systems.
- There has been direct cost saving to citizens in the range of Rs.50-100.
- In Land Records project, there has been a significant reduction in the payment of bribes

5.1.4 Income Tax Department (ITD)

Central Board of Direct Taxes (CBDT) has undertaken a business process Re-engineering project under the leadership of the honorable finance minister of India. A new directorate of Income Tax has been set up at New Delhi for this purpose. The objective of this project was to:

- Re-evaluate all existing processes and procedures to determine future direction
- Focus on how organizations can meet the requirements of stakeholders
- Use leading practices in other organizations to develop milestones, objectives, targets to benchmark organization results and redesign new processes
- Simplify and empower the organizational structure
- Increase alignment between process, people and technology
- Change Management and Capacity Building

The overall scope of work for the project was to:

- Review the overall strategic framework and vision of the department keeping in mind basic functions of the department
- Redesign processes across all activities of the Income Tax Department based upon international leading practices and unique requirements and limitations of the Indian Tax Administration system
- Identify improvement opportunities, quick wins and a transition plan for implementing the
- BPR recommendations including the changes and resources required to implement
- Detailed change management measures, especially for changes recommended in organizational design as a corollary to the implementation requirements of the redesigned process
- Suggest changes in physical IT infrastructure in line with the new business design The services that are being delivered as part of this assignment are as follows:

Business Process Re-engineering

- Study of existing business processes in four strategic process areas namely Pre-Assessment, Assessment, Post-Assessment and Appellate
- Study of international leading practices in other countries with respect to the Income Tax services being delivered
- Collection of baseline data in eight cities to statistically support the issues and opportunities identified in the current business processes
- Gap analysis and design of "To-Be" processes. Conduct process redesign workshops with stakeholders in Income Tax Departments

Assessment of Taxpayer Perception

- Voice of Customer Survey in eight cities across various offices of the Income Tax Department to assessment

Institutional Analysis

- Study of existing manpower and capacity building requirements to support the re-engineered processes
- Develop an organizational structure including functions, roles and responsibilities, job requirements, job roles etc.
- Assessment of organizational strengths and weaknesses
- Evaluation of change readiness assessment within the department
- Development of a flexible change management plan to transition the entire organization
- Study of existing technology infrastructure and analysis and design of technology enablement plan to suit the needs of the re-engineered organization

Training

Training needs assessment to improve skills, raise awareness and to communicate requirements of ITD's change initiative goals to both internal and external audiences.

Develop Implementation Strategies.

Selected strategies needed to be agreed upon to support the construction of the changed or new policies, processes, organization, technologies and facilities.

Develop Implementation Plans

Migration plans and detailed implementation plans were prepared to support migration to the changed environment. The BPR report had among other things:

- An implementation approach for "quick wins" identified earlier
- Changes identified in the business rules and processes

- Submission of implementation plan

5.2 e-Governance Success Stories (State Sector MMPs I Projects)

5.2.1 Integrated Land Information System (ILIS) for Andhra Pradesh

Existing System of Land Records

- Legacy of British System
- Land Records created mainly for 'Land Revenue'
- Based on 'Presumptive Ownership'
- Processes & services, mostly manual
- Managed by multiple agencies
  - Survey and Land Records: FMB/ Tippon, Village Map, Shetwar/RSR
  - Revenue Department: ROR Register, Adangal/Pahani, Pattadar Khata Register
  - Stamps & Registration: Register of Transactions (Book 1-4, & Indices)
  - Local Bodies: Town Survey Register, Town Survey Maps, Layout plans, Property tax register

Land Records - Concerns

- 'Registration' does not confer 'Title'
  - Insecurity about Title - Loss estimated at 1.3% of GDP, due to unclear land titles
  - Title and boundary disputes - Costly litigation
- Registration & Land records - Stand-alone systems
- Multiple handling agencies - Lack of co-ordination
- Non-availability of up to-date records - Developmental and planning activities affected

Vision of ILIS

'To establish and manage a comprehensive and sustainable Land Information Management System, which serves as a record of conclusive title of all land parcels and provides related services in an integrated, efficient and cost effective manner.'

5.2.2 Transport

- 'Sarathi & Vahan' are under implementation in various Stages in many States. 'Sarathi & Vahan' provides total automation of Regional Transport Office transactions comprising of Fee and Tax, all stages of Registration, License, Permit and Enforcement, Fitness, Fee and Tax sections through workflow based system.
- Several States including Delhi, Gujarat, Maharashtra, MP, etc. are issuing Smart Card Driving Licenses.
- In Andhra Pradesh, CFST (Citizen Friendly Services of Transport Department) is already implemented under PPP Model in all 38 offices with 400+ counters across the State.
- In Tamil Nadu, State government has set up a modern control room at the state traffic planning cell (STPC) office on Kamarajar Salai to monitor the 122 GPS-enabled police patrol vehicles deployed along the national highways across the state. The system helps the police patrol vehicles to reach the accident spot within two minutes of the incident.

5.2.3 e-District

e-District is a State Mission Mode Project under the National e-Governance Plan (NeGP). The project aims to target high volume services currently not covered by any MMP under NeGP and undertake backend computerization to e-enable the delivery of these services through Common Service Centres.

Districts are the primary delivery channels for government administration which delivers a large number of services to the citizens; therefore e-Governance can significantly improve government service delivery.

Objectives of e-District:

- To integrate and seamlessly deliver citizen services by district administration through backend digitization and process redesign
- To create an efficient delivery mechanism from the Government that brings citizens to the district administration
- Implementation of an efficient electronic workflow system for reduction of workload of the district personnel
- To create a smart link/interface between citizens, governments, public utilities and other information providers
- Fast processing of public cases/appeals/grievances dissemination of information
- Focus is on backend computerization

e-District will primarily focus on the back end computerization and use the SWAN for connectivity and CSC for service delivery. The main focus would be on ensuring that the project is self sustaining after the initial investment. This is possible if revenues generated from services are available at the district level for maintenance, upgradation and expansion.

5.2.4 Excise / VAT

The Department of Excise & Taxation introduced e-Governance by leveraging ICT to streamline Tax Administration and improve upon its functioning in order to bring efficiency, transparency and accountability.

The objective of the project is to establish an ICT system with focus on:

- Implementation of an electronic workflow system to improve internal administrative efficiency
- Faster processing and monitoring resulting in better and transparent delivery of service to the tax payers,
- Backend computerization of the functions of the Department
- Standardization of commercial tax administration across the State,
- Introduction of a bouquet of rationalized citizen-centric and service-oriented processes
- Enhancement to the quality of services provided to citizens
- Addressal of public cases / appeals / grievances with service levels
- Dissemination of information as per public requirement
- Plug-tax loopholes and foster a citizen-centric dispensation aimed at better compliance
- Increase the tax payers base
- Strengthen the government's revenue base
- Establish a real-time MIS system for prompt and efficient decision making
- Suggest improvements based on innovations, initiatives and best practices from similar systems

6. e-Governance Vision and Strategy

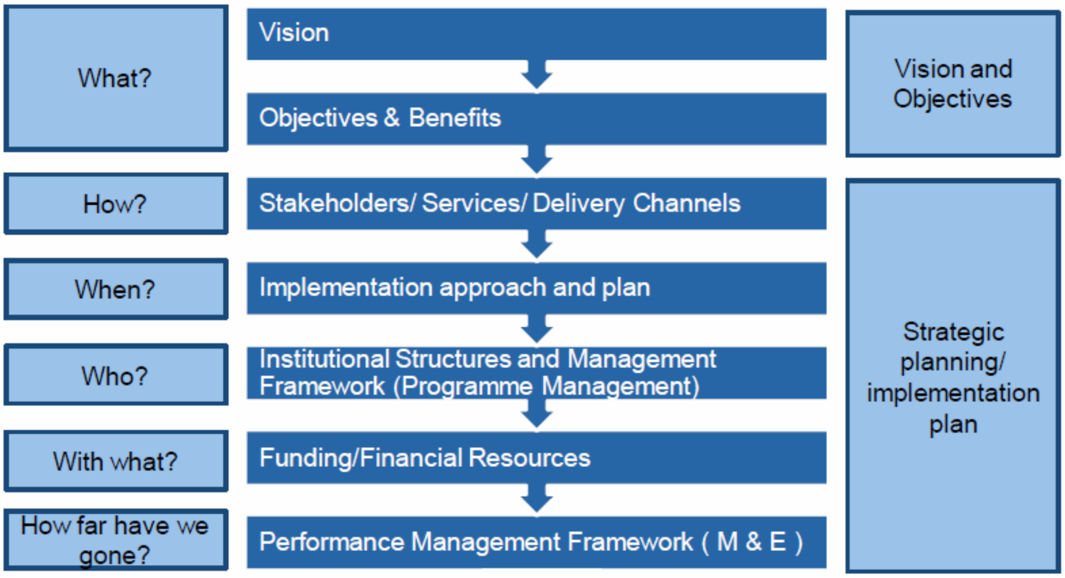
6.1 Understanding e-Governance Strategy

'Strategy' in simple terms is a plan of action for achieving the defined goals and objectives and is a road map to lead an organization from its present state to its desired medium or long term future state. 'e-Governance Strategy' is an approach or a plan of action stating how Information Technology will be leveraged in achieving the stated goals and objectives. e-Governance strategy is needed to:

- Provide direction and guidance in IT adoption
- Clearly identify the clear and measurable benefits from leveraging IT
- Clearly identify the actionable and measurable initiatives for achieving the stated goals / benefits
- Estimate the resources (people, funding..) needed for
- Maximize effectiveness of ICT initiatives within Government
- Effectively plan and utilize the resources to gain maximum results
- Map path from pilot experiments to sustainable, scalable systems
- Key considerations for development of e-Governance strategy include:
- Ensure consistency with economic development priorities
- To keep the business goals and objectives on priority, not the 'technology'
- To pursue real development goals not just "technology push"
- Secure political support
- Establish stakeholder participation mechanisms (including demand)
- Secure stakeholder buy-in of implementation plan

6.2 Key Elements in e-Governance Strategy

Diagram below summarizes the key elements of an e-Governance strategy and following paragraphs discusses each of these elements in summary.

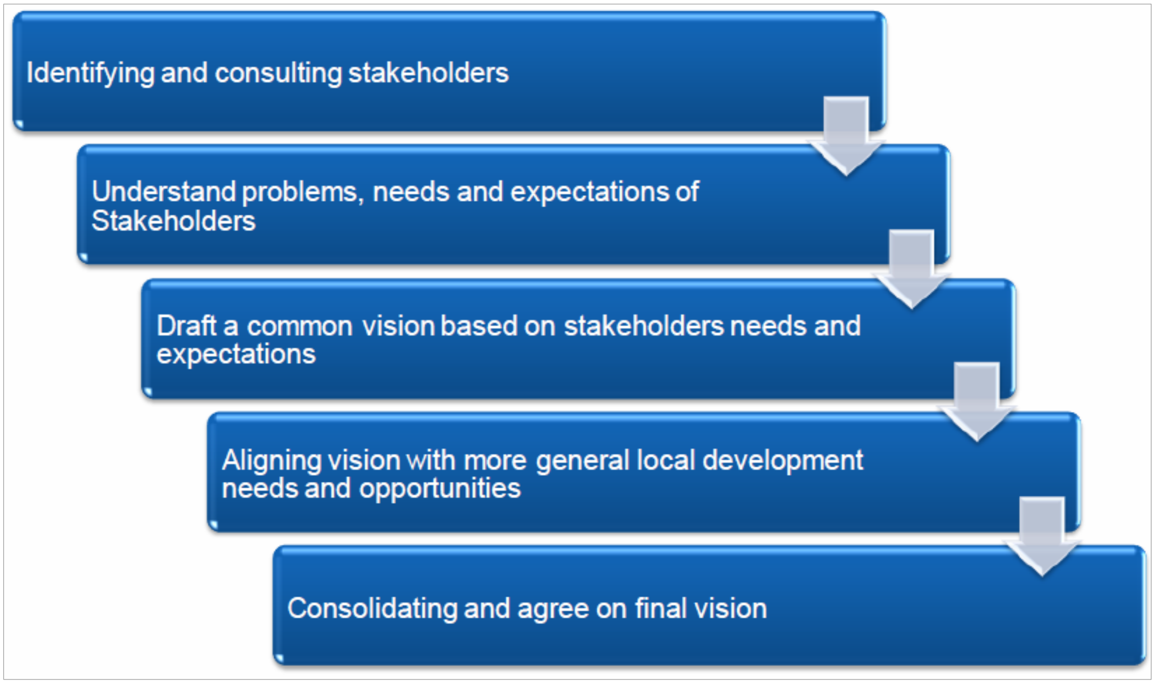

What?
Vision
Objectives & Benefits
Vision and Objectives
How?
Stakeholders/ Services/ Delivery Channels
When?
Implementation approach and plan
Who?
Institutional Structures and Management Framework (Programme Management)
With what?
Funding/Financial Resources
How far have we gone?
Performance Management Framework (M & E)
Strategic planning/ implementation plan

6.2.1 e-Governance Vision

Vision is a succinct and inspiring statement of what the organization intends to become and to achieve at some point in the future. Before embarking on one or several e-Government projects, government should make sure that there is a vision that provides a roadmap and guidance for institutional change. A vision statement takes into account the current status of the organization, and serves to point the direction of where the organization wishes to go. The vision statement provides the direction for the organization, while not inhibiting the development of the strategy that will allow the organization to reach the desired goal. It is not about 'automation' or 'computerization'. It is about 'what' will be achieved using IT and should be inline and supportive of organization's business vision. A vision statement should:

- Be clear, intuitive and simple
- Reflect the specific conditions and ambitions of the organization
- State what will be and will not be done
- Consider needs and opportunities
- Be aligned with overall development strategy
- Involve consensus building by stakeholders

Following diagram presents an overview of approach for development of e-Governance vision.


Identifying and consulting stakeholders
Understand problems, needs and expectations of Stakeholders
Draft a common vision based on stakeholders needs and expectations
Aligning vision with more general local development needs and opportunities
Consolidating and agree on final vision

Examples of e-Governance vision include:

a) "Use e-Government solutions as the primary delivery channel to provide a single, easy, integrated, and reliable means of access to Municipal information and services in order to continuously improve the quality of services provided for the residents, businesses and partners, reduce internal operational overhead, enhance revenues and promote Dubai's image as a commercial and tourism hub in the Gulf region."

b) eBiz - Establish One-stop-service delivery centre for G2B Services in India, provide services in simplified and convenient manner and thereby improving the investment climate in the country

c) e-Procurement: Establish common procurement platform for realizing the right value for the goods & services, minimizing the cost of procurement and providing equal opportunities for businesses.

d) NeGP Vision - "Make all Government services accessible to the common man in his locality, through common service delivery outlets and ensure efficiency, transparency & reliability of such services at affordable costs to realize the basic needs of the common man."

e) e-Governance Vision of Canada - Using information and communication technology to enhance Canadians' access to improved citizen-centred, integrated services, anytime, anywhere and in the official language of their choice

6.2.2 e-Governance Objectives

An objective is a specific and usually quantifiable statement of program achievement and is a statement of measurable outcome which can be used to determine program progress towards the goal. Collectively, objectives represent a quantification of the program goal. e-Governance objectives translate the broad values within a vision into more real and tangible outcomes, with stronger operational basis, reflecting actual process, procedures and measurable outputs. Objectives should have measurable criteria for achieving success

e-Government does not differ from any other business endeavor/objectives and e-Governance objectives should flow from e-Governance vision. e-Government should not be considered as a business goal or objective by itself rather, it is a means to achieve business goals or objectives. Accordingly, e-Government objectives should be established along two dimensions (i) Adding benefits to the customers and (ii) Adding benefits to the organization itself. The most effective business objectives are often generated from your existing business strategy and e-Government business objectives are usually driven by global reach, customer self-service and effective information sharing.

Defining e-Governance Objectives (illustrative)

For Citizens (General / ambiguous Objectives)	**For Citizens (Specific Objectives)**
• Streamlined, standardized electronic information gathering and access • Reduce the time to access relevant information • Enable citizens to find benefits and determine eligibility • Reduce the time for citizens to find information on opportunities, schemes, benefits etc. • Electronic delivery of services • Convenient, any time and anywhere services • Convenient & simplified processes for establishment, operations, expansion of businesses • Minimize burden on businesses through online forms/services • Reduce time for filing and complying with regulations • Increased and equal access to business opportunities with Government	• Provide Passport to citizens in 3 business days • Instantaneous payments of taxes & bills online through kiosks • Instantaneous access to Information Services • Business Registration in 5 Working Days • Online Filing of Returns etc.

For Department (Broad Objectives)	**For Department (Specific Objectives)**

• Reduced administrative burden and Increased employee productivity • Information reuse across and within departments • Cost effectiveness in operations	• Minimize direct interaction between department & citizens • Reduce cost of procurement by 50% • Migrate to 75% online service delivery by 2008 • 0% of transactions at Department counters for payment of taxes, duties etc.

Key Considerations for Vision and Objectives Definition:

- To be developed based on extensive interactions with stakeholders, not based on board room discussions
- To be developed from stakeholder needs, not by department thoughts
- Stakeholders include:
    - Customers (citizens, businesses..) served by the government
    - Employees of organization delivering the services..
- To be developed to address the current challenges and future needs
- To take learning / inputs from similar situations and initiatives in India and world wide.

6.2.3 Identifying Stakeholders/Services/Projects/Delivery Channels

a) Stakeholders

Clear identification of stakeholders and related benefits is a key requirement for a successful implementation of e-Governance projects. Following discusses the typical stakeholders in e-Governance projects.

- Customer Segmentation
    - Citizens
    - Businesses
    - Partners (suppliers and other government agencies)
- Key Customer needs to be considered
    - Easy Access - single & reliable access to information & services
    - Clear Accountability - for delivering the services
    - Integrated view of customers - no longer be required to submit the same information / documents repeatedly

Priorities/Benefits sought by various stakeholders (illustrative)

People as Citizens/ service users	Businesses	Public administrators (employees)
• Accessibility • Ease of use	• Cost-effectiveness	• Empowers employees
• Confidentiality • Privacy	• Resource rationalization • Value for money	• Reduced admin burden
• Transparency, openness • Trustworthiness	• Economic growth • Productivity	• Continuity and stability • Easy to use

b) Services

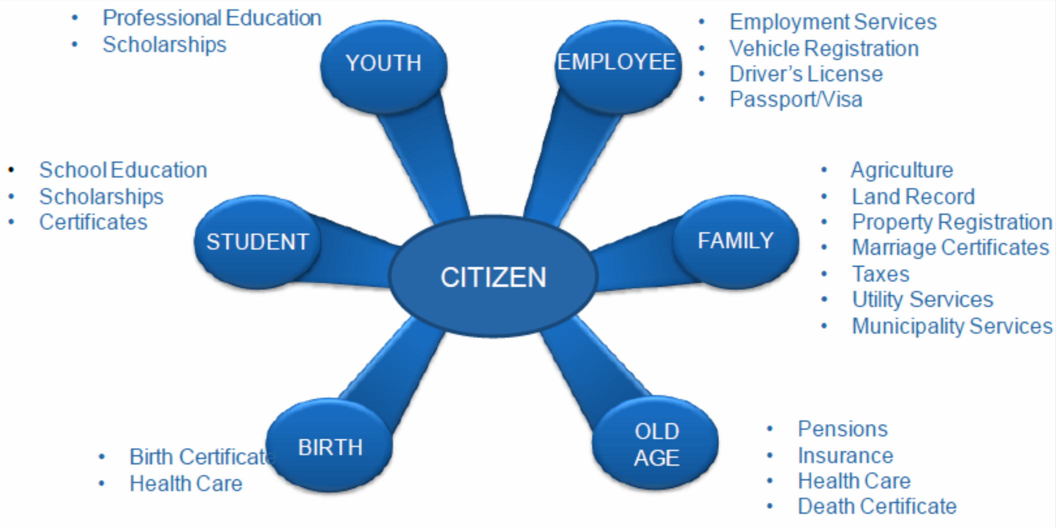
Service is the 'action or process of serving' or 'an act of assistance' or 'a system providing a public need'. Process consisting of a series of intangible activities that normally, but not necessarily always, takes place in interactions between the provider and consumer. Government is into the business of addressing the needs of citizen through the Lifecycle and Governments interact with citizens to provide 'services'. Every government department provides a set of services to its identified customer base. The delivery of such services would develop an image of the government among the customers and so making the delivery of services customer-friendly.

Categories of Government Services:

G2C	Government to Citizen
G2B	Government to Business
G2E	Government to Employee
G2G	Government to Government

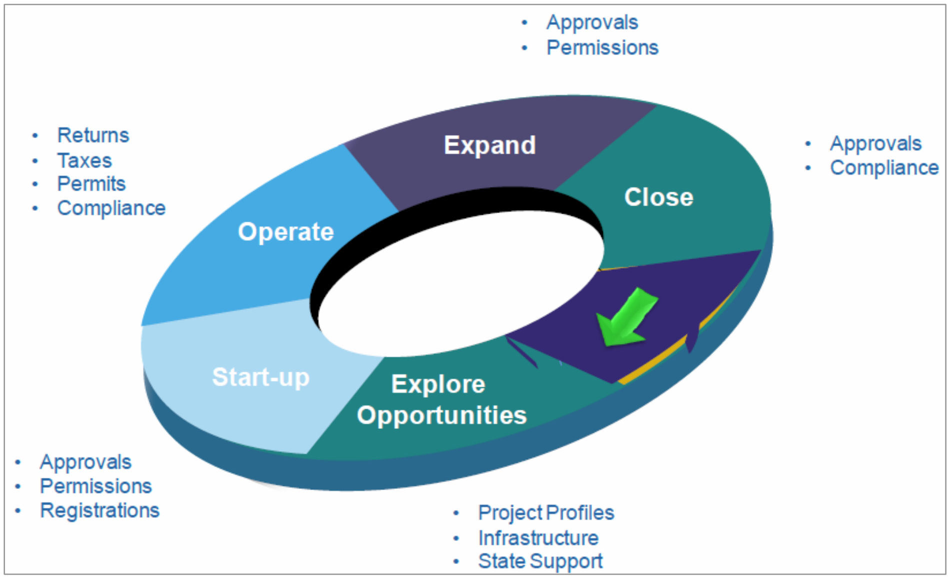
G2C Services:

Diagram below outlines various government services provided across the Lifecycle of a citizen.



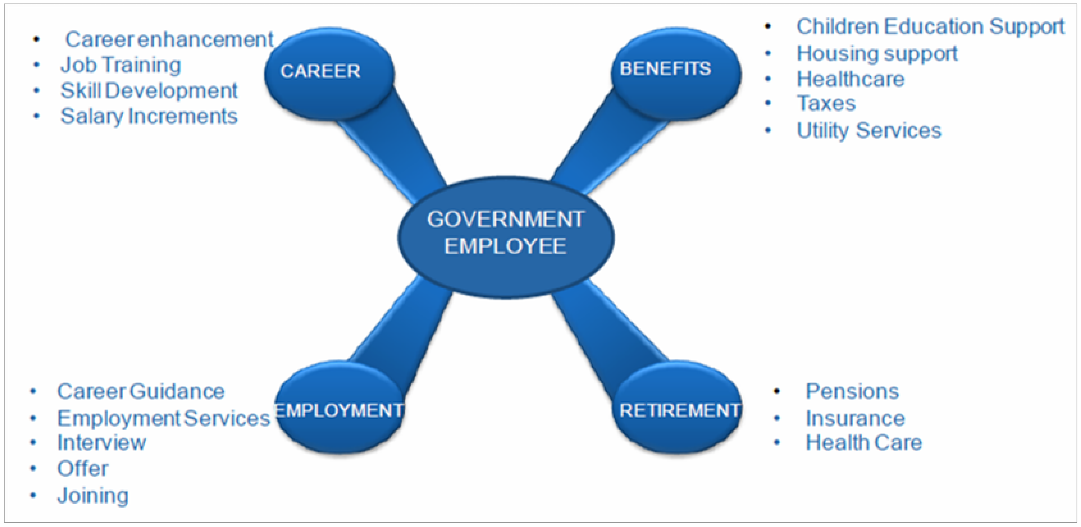
G2B Services:

Diagram below outlines various government services provided across the Lifecycle of a business.



G2E Services:

Diagram below outlines various government services provided across the Lifecycle of employment with government.



The services of the government are generally classified into information and transaction services:

• Information Services

- Includes those services that solely provide 'information' to customers and does not involve processing of any transactions or documents.
- Information services have relatively simple back-office operations and can be easily be e-Government-enabled

• Transaction Services

- Transactional Services: includes those services where customers require specific actions to be taken by the department.
- Transactional services mandate a higher degree of customer interaction and more complex delivery operations than informational services.

Service Prioritization

Several e-Governance initiatives at central/state/local government undertaken and significant investments made in IT enablement in various departments along with several years of time and efforts of government and private sector consumed. However, the benefits and results in many of the projects are minimal as the governments have adopted implementation of e-Governance across the functions and services in one go and this approach many a times have failed in achieving the benefits. Key reasons for such failures include:

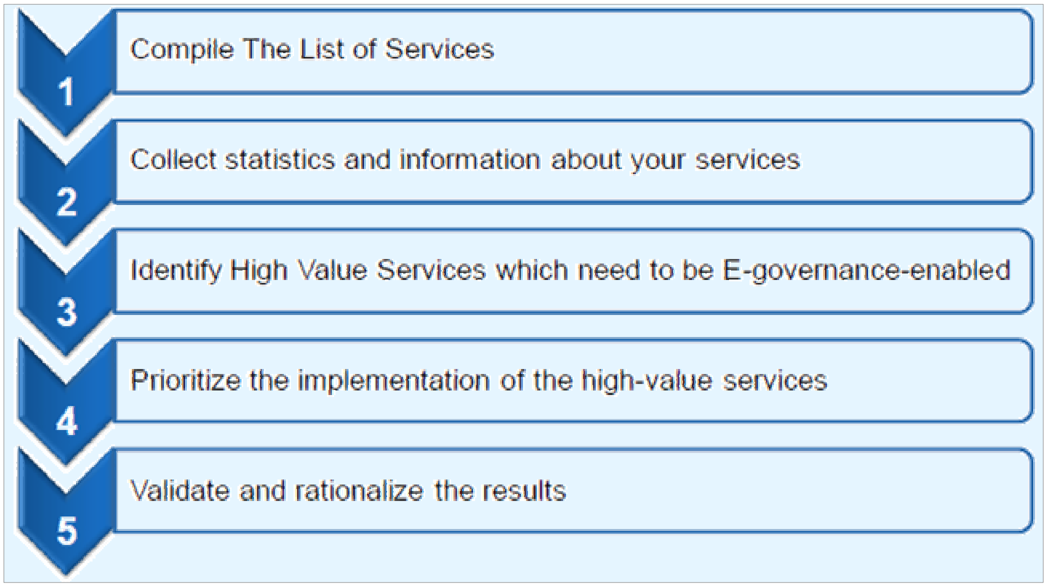
- Most projects are undertaken as automation of department functions/workflows - lack of services view
- Lack of citizen/customer centricity in projects design/approach
- Lack of 'services' point of view in project design
- Departments have undertaken organization wide computerization at one go - leading to significant efforts with minimum/delayed results
- Project sustainability impacted due to large size and complexity of engagements not delivering results for long durations
- Limited resources, skill sets - lack of capacities and skill sets to manage large and complex

IT projects leading to project failures/takeoff

Prioritization of services and ICT enablement of these services in a phased manner can enable the organization to invest the managerial efforts in successful management of implementation and in addressing the risks and issues during the implementation. The need for the service prioritization includes:

- To demonstrate early results
- To minimize the impact and maximize the results
- Limited resources and capacities existing with (funds and skill sets)
- Lack of readiness of stakeholders

Following outlines the approach for service prioritization:


1
Compile The List of Services
2
Collect statistics and information about your services
3
Identify High Value Services which need to be E-governance-enabled
4
Prioritize the implementation of the high-value services
5
Validate and rationalize the results

Step 1: Compile the list of services

- Identify the stakeholders addressed/served by the department
  - First level of classification (citizens, businesses, employees, other governments)
  - Sub-classification (e.g. of citizens served by Education Dept) - Parents, Higher education level students, university level students, private college owners.
- Identification of department functions/services to the stakeholder groups
- Identification of list of information and transaction services stakeholder wise

Step 2: Collect information & statistics about the various services

- Collection of various operational information and statistics for the list of services identified in Step 1
- Illustrative Information and statistics for each service include:
  - Transaction volumes
  - Frequency of transactions
  - Transaction processing time
  - Number of customer visits
  - Time spent by the customer for follow-up and track progress
- Illustrative analysis of Municipal Services

Service	Transaction volumes (per year)	Frequency	Processing time
Birth registration	10,000	Once in lifetime	1 day
Death registration	4,000	Once in lifetime	1 day
Property tax assessment	3000	Once in lifetime	2 days
Property tax collection	100000	Twice in a year	30 minutes
Issuing building permission	1000	Once in lifetime	10 days
Vacant Land Tax Assessment	10	Once in lifetime	2 days
Vacant Land Collection	100	Once in a year	30 minutes
Court cases	10	NA	
Water tap connection	1000	Once in lifetime	2 days
Water tax payment	250000	Once in a month	30 minutes

Step 3: Identify High Value Services Which Need To Be Transformed Into e-Governance

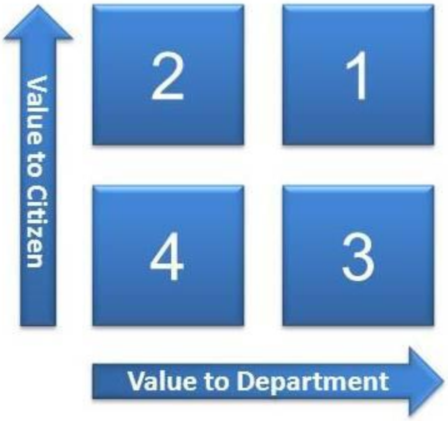
Assessment of services to identify those services that once made e-Governance-enabled will deliver the maximum value to the 'department' and its 'citizens'.

Department Value Measures	Citizen Value Measures
• Enhancing existing revenues; • Setting up new revenue streams; • Reducing cost of processing transactions; and • Delivering intangible benefits (e.g. boosting the image of the department)	• Minimizing the number of customer visits • Reducing the time required for service • Reducing the fees and charges associated with a service; • Reducing the time spent by the customer to follow-up and track the progress • Reducing the time spend by the customer to file complaints, comments and suggestions

Measures for Value to Citizen	Measures for Value to Department
• Minimizing the number of customer visits to the department • Reducing the time required to deliver a service • Reducing the time spent by the customer for follow-up and track progress of the requested service • Reducing the time spent by the customer to file complaints	• Reducing cost of processing transactions • Delivering intangible benefits • Increase transaction volumes

Identification of high value services:

Diagram below presents the four box model, which can be used for identification of high value services. Services falling in to box 1 are high value services to both citizen and the department and needs ICT enablement on a priority basis followed by others.



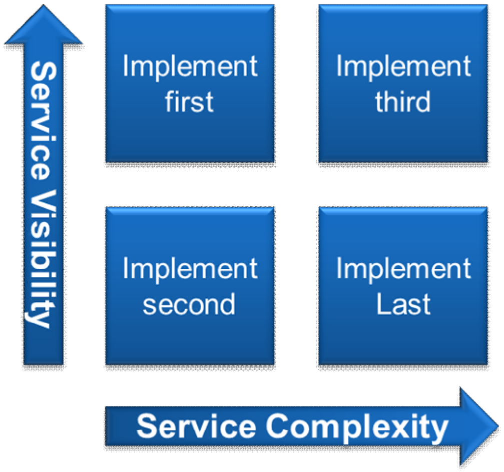
Step 4: Prioritize Implementation of High Value Services

- Identify when to implement each of the high value services identified for the department
- The implementation priority for each high value service is defined based on the analysis of service visibility and service complexity

Service Visibility	Measures for Service visibility
• Describes how significantly and extensively can customers feel and experience the benefits achieved from delivering the service into e-Governance. • Services of high volume of transactions and a large customer base would be more visible to the Department customers than other services with a very limited customer base	• Volume of transactions • Customer base • Intangible benefits

Service Complexity	Measures for Value to Department
• Describes how easy the service can be made e-Governance-enabled. • Depends on a number of factors such as the degree of existing automation, number of external parties involved and the number of customer documents processed	• Degree of existing automations • Number of external agencies involved • Number of customer documents processed

Following diagram provides approach for prioritization of high value services.



Step 5: Validate and Rationalize the Results

- Validate the identified services/projects for e-Governance through department's survey, experience and knowledge of the customers
- Verify whether high-value services can deliver benefits through e-Governance.
- Verify the feasibility of the implementation priorities assigned to the high-value services

Benefits of Service Prioritization:

- Identifies the services which are crucial to the stakeholders and which requires immediate IT enablement
- Enables process efficiency to the high priority services
- Increased user value and satisfaction
- Reduced administrative burden
- Strategic Fit with e-Government strategy
- Increased visibility of efforts and benefits

c) Delivery Channels

Selection of delivery channels is a critical element. Identifying portal and internet as a service delivery channel as the primary channel for citizens in rural parts of the State is a bad choice as Internet penetration in villages and rural parts is LOW. Selection of right and appropriate service delivery channel, based on target stakeholder group, determines the project success. Following lists some key service delivery channels for various stakeholder groups.

- Channels
    - Department counters
    - Internet/Portal
    - Call Center
    - Kiosk (CSCs)
    - Mobile computing etc.
- Primary Channels
    - Internet & Kiosks
- Secondary channels
    - Call Center & Department Counters
- Extended Reach
    - Mobile computing etc.

6.2.4 Implementation Approach and Plan

The four most widely discussed implementation models are:

- **Big Bang** - The e-Governance project is launched across the locations for all the functions at the same time. All users move to the new system on a given date.
- **Phased rollout** - Changeover occurs in phases over an extended period of time. Users move onto new system in a phased manner.
- **Parallel adoption** - Both the legacy and new system run at the same time. Users learn the new system while working on the old.
- **Pilot and rollout** - A small (sample) part of the project is implemented for testing purposes before the complete project rollout is done.

a) Big Bang Approach

- The rollout happens in a single, major event. It means:
  - Roll out of all modules/functions of system at the same time
  - Roll out to all categories of users at the same time
  - Rollout to all locations/geographies at the same time
- Requires significant pre-implementation work, planning and stringent implementation monitoring and control to ensure project success
- The most common criticism in the big bang implementation strategy is the risk factor; there are a number of things that could go wrong in an instant changeover
- If successfully performed, it may minimize the impact, elapsed time and cost as the implementation is quick and less costly than a long, drawn-out phased approach
- From earlier experiences, the likelihood of success in a big bang approach are comparatively less

Following compares the advantages and disadvantages of big-bang approach.

Advantages	Disadvantages
• Implementation time is shorter • Implementation difficulties and "pains" are condensed • Costs are much lower than a long, drawn-out implementation • Implementation happens on a single date and everyone knows the date.	• Difficulties are more pronounced • Details may be overlooked in the rush to change • Employees have less time to learn the new system • Full end-to-end system testing is tough to carry out prior to implementation • Fall-back scenarios are more difficult than originally perceived • A failure in one part of the system could affect others • If any issue arises, the multiplier effect of the issue is much higher considering geographical spread and no of users

b) Phased Rollout

- Phased rollout would be analogous to the Steady State theory: instead of an implementation happening in a single instance, small changes occur over time
- An organization moves off the legacy system and onto the new system in a series of predetermined steps
- This can be achieved in several different ways along the following four key dimensions:
  - By business functions/ module
  - By locations/geography
  - By size and value of transactions (e.g. in case of e-procurement high-value

procurements can be run through the system for testing)

- By category of users

Phased Rollout - by functions/module	Phased rollout by geography
• Based on the service prioritization approach • High value and low complexity services/functions are implemented first to gain maximum benefits from IT followed by others • Facilitates better utilization of resources for e-enabling high-value services.	• The applications/services are implemented in a small number of locations first • Aimed at testing the functionality of the system/services in the field/real life environment and to address the gaps before it is rolled out to other locations • Commonly adopted approach for large organizations that have presence across large/multiple number of locations (many government departments have similar spread)

Following compares the advantages and disadvantages of phased rollout approach.

Phased Rollout - by functions/module	Phased rollout by geography
• Organizations gain knowledge and experience during the initial implementation phase that can be applied to subsequent phases • Possible to introduce some modules first without waiting for the entire systems development phase for all modules to be completed • With conversion occurring in parts, time is available for adjustments • Minimizes impact of gaps/issues identified in the system (expected to be corrected before rollout) • Manageable number of issues and complexities • More time for users to adapt to the new system • Technical staff can focus on one part of the system or a select group of users at one time - enhanced focus. • Project members may develop unique implementation skills that they can be positioned for in later rollouts	• Involves continuous change over an extended period of time • Duration of the project is much longer than big bang • Temporary bridges must be created between legacy system and new system considering phased migration of functions from old system to new system • Need to maintain sustained interest from management and users throughout implementation • Needs repetition of cycle multiple times. testing, training

c) Parallel Rollout

- It is a method for transferring between old (IT) systems to a target (IT) system in an organization.
- In order to reduce risk, the old and new system run simultaneously for some period of time after which, if the criteria for the new system are met, the old system is disabled.
- Parallel adoption is thought to be the least risky implementation process.

The parallel adoption process cannot be represented without paying attention to the following steps before the actual conversion, namely the construction of a conversion scenario and the identification and testing of all the requirements. The activities are divided in three main phases:

- **Define implementation strategy:** deals with the kind of implementation strategy should be executed.

- **Prepare organization:** The organization should be prepared properly according to the previous phase.
- **Conversion:** deals with the actual conversion process and closing the conversion process; proceeding with the new system.

Disadvantages of Parallel Rollout

- Parallel adoption is the most expensive implementation method.
- Having employees enter data in both systems is not efficient.
- Organizations cannot predict cost overruns of big bang, so parallel adoption has become decreasingly popular because of perceived high costs.

6.2.5 Program Management Framework

- A well planned program or project management office with right resources, skills and infrastructure can substantially improve the likelihood of project success
- Program management office should consist of cross-functional teams with direct and strong executive management support e-Government implementation efforts are generally distributed as follows :
  - 10% technical infrastructure implementation
  - 30% software development and system integration
  - 50% change management
  - 10% other activities
- Change management should focus on four key people segments - suppliers, business partners, customers and employees.
- Program management should appoint strategic partners for advice and counseling on technical and business issues.
- Program management should follow a phased approach with clear deliverables and regular check-points.

Departments should work towards institutionalizing the program management offices/structures into a permanent e-Governance functions/structure within the organization with exclusive focus on e-Governance & should focus on building capacities for these teams to takeover program management functions and roles from private sector in a long term basis.

6.2.6 Funding and Financial Resources

Business models for e-Governance projects are discussed in detail in the later sections

6.2.7 Performance Management Framework (M & E)

M & E framework need and approach for e-Governance projects has been discussed in detail in later sections.

7. Government Process Re-engineering (GPR)

7.1 e-Governance and Traditional Approach to e-Governance

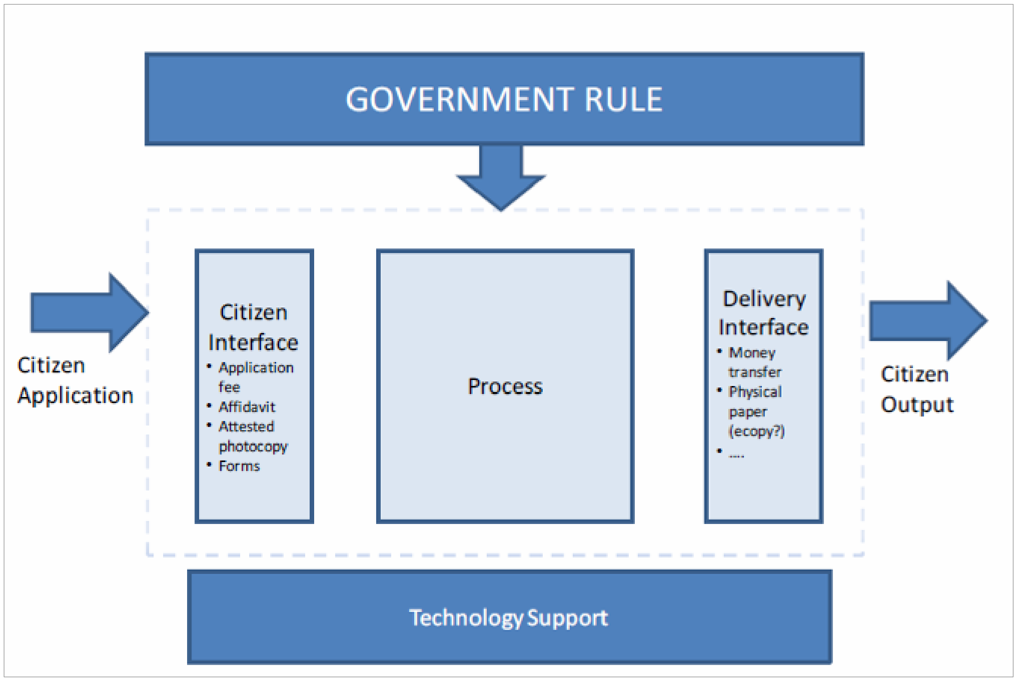
Over the past few years the concepts of government and governance have been dramatically transformed. Not only is this due to increasing pressures and expectations that the way we are governed should reflect modern methods of efficiency and effectiveness (that governments should 'do more for less' year on year), but also that government should be more open to democratic accountability.

There is an increased emphasis of usage of ICT in the delivery of public services in a more efficient and effective manner. But the usage of new technologies goes much further. They are starting to redefine the landscape of government by changing the relationships (power and responsibility) between players - between service providers and industry, between the public, private and third party sectors, and between government and citizen. Hence ICT can make government transformational - creating and retaining the capacity and capability to innovate and use technology effectively as technology develops.

It is vital that the process redesign, i.e. the critical analysis and radical redesign of workflows and processes within and between governmental departments, is undertaken if we are to achieve breakthrough improvements in performance.
Hence the key to a good BPR is redefining processes to facilitate the citizens / user convenience

Innovativeness: It should think innovatively and come up with solutions rather than replicating the manual system.
Transformational: It should bring about a drastic improvement in the quality of services provided.
Rationalization of Application form and data requirements: Very often the information asked for in the application is rarely used or is already available with the Government. A good BPR would question the need of all information sought.
Usage of data available in Government domain efficiently: Very often the information sought is available in the Government domain. Date of birth is an example of commonly sought information. This is to be generally supported with a duly attested certificate as proof. This may be done away with as the Government already has the information through date of Birth records of the individual. Hence asking for a Birth Certificate is a redundant activity.

Very often there is a misinterpretation of a government rule with a government procedure. At an operational level, it is often thought that the procedure is the rule. For example let's say that a pension is allowed for people above the age of 6S.This is a rule. However to prove that a person is 6S there could be various options available like Class 10th pass certificate, Birth Certificate, Passport etc. This is a procedure.



In a BPR one has to differentiate between a government rule and a procedure. Very often it is seen that procedures can be completely revamped through the use of IT. Like in the above case, these documents are not required if the access to birth data is provided to the concerned officials requiring this proof.

7.2 Re-engineering defined

The Re-engineering of governmental processes is a necessary condition for the realization of the benefits of e-Governance. The importance of process redesign to facilitate and ensure best practices in the realm of e-Governance needs to be emphasized. It is vital that the Process Redesign involves the critical analysis and radical redesign of workflows and processes within and between governmental departments to achieve breakthrough improvements in performance. While deployment of IT solutions increases the efficiency of operations, it will not necessarily deliver the best results unless the processes are reconfigured to the most appropriate processes given the demands of the specific circumstances. Otherwise, there is always the threat that replacement of manual processes by machine-based processes will only lead to "automated" waste. Process Re-engineering ensures that the processes are redesigned to make them the most effective and deliver the maximum value to the government, its employees and the last but not the least the common citizen.

The experience of some of the Governments shows that real crux of convergent/integrated delivery of public/private services lies in Re-engineering of government/business processes (40%) and change management (45%) rather than technology including hardware and software (15%).

"Re-engineering is the fundamental rethinking and radical redesign of business processes to achieve dramatic improvements in critical, contemporary measures of performance, such as cost, quality, service, and speed." -Hammer and Champy, 1993

It is often not possible to wipe the slate clean and start afresh at redesigning a business or process. Six Sigma's DMAIC methodology offers a methodology for taking existing processes to new heights and may include a measure of redesign.

Design for Six Sigma (DFSS) on the other hand offers a methodology that is specifically geared at creating new processes and offerings.

SIX SIGMA is a structured methodology that can be used to improve the quality of service and performance. Once we know the actual performance level for any services using six-sigma methodologies, we can improve that performance level. Following diagrams gives the details on the two commonly used techniques for improving process using six sigma methodologies:

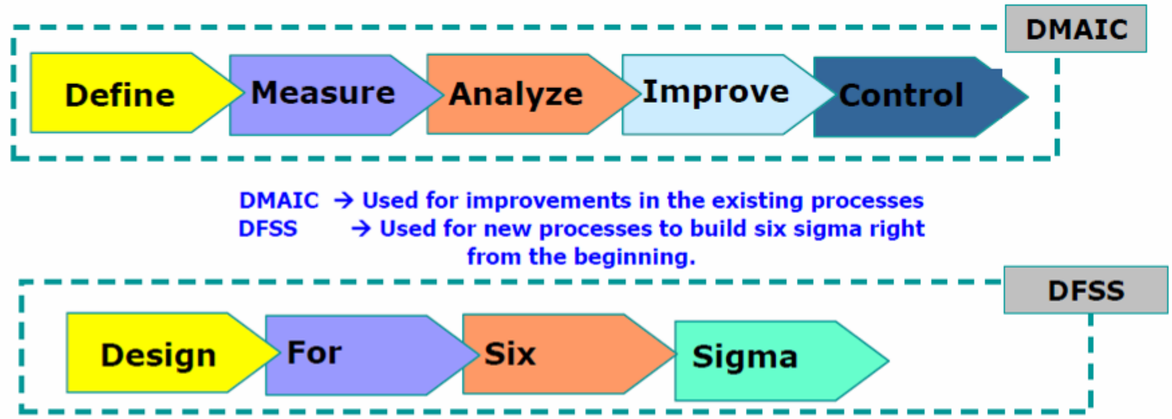

DMAIC
Define
Measure
Analyze
Improve
Control
DMAIC → Used for improvements in the existing processes
DFSS → Used for new processes to build six sigma right from the beginning.
DFSS
Design
For
Six
Sigma

Figure 1: Six Sigma Methodologies

Six Sigma brings to BPR the following elements:

- Proven set of statistical tools and methods to eliminate variation
- Data driven design or improvement
- Use of scorecards, dashboards, metrics and baselines
- Stage gating to ensure initial assumptions are valid while maintaining vigilance for changes
- Elimination of waste time, effort or resources
- All efforts are linked back to the 'Voice of the Customer', the business strategy and objectives

7.3 BPR (GPR)

Re-engineering is also consistent with the new form of governance that has emerged during the Information Age-one that favors mission-driven, results-oriented activities. Even with this new focus, there are some elements of the public sector that will not change and remain challenging for Re-engineering implementers. For instance, government agencies are subject to greater political executive management and oversight. Election cycles and administration changes also affect Re-engineering efforts. In addition, governments cannot revise or depart from their missions and operations, whereas in the private sector there is much greater discretion to change business orientations. Legislation, taxpayer accountability, competition for funding and resources, continuous change, as well as partnerships with international, state, and local governments will continue to challenge government agencies as they reengineer. Perhaps the most critical challenge for government lies in the area of risk-taking. Historically the culture of the government has been to avoid risk. Any successful Re-engineering effort will need to embrace change and negotiate some degree of risk.

There is a great deal of experience in Business Process Re-engineering. But the government is not a 'business'. Because businesses have to perform such Re-engineering of legacy systems, and because they face similar difficulties, it is tempting to treat government as a large business in the analysis of the problem. However, government has many drivers and difficulties of context that businesses do not face: in particular, whereas businesses have the (relatively) straightforward goal of creating value for shareholders within the law, governments need to meet a wide range of targets. Government remains distinctive from business for many reasons, including the fact that government cannot choose its customers and that user of government services take on a variety of roles, including as voters, taxpayers as well as consumers. Thus, a 'government process Re-engineering' (GPR) approach may be more appropriate, learning from, but also informing business (for example in terms of social responsibility), in the context of public, private and non-profit sector partnerships.

The National Academy of Public Administration, USA, recast the definition of Re-engineering for government:

"Government business process Re-engineering is a radical improvement approach that critically examines, rethinks, and redesigns mission product and service processes within a political environment. It achieves dramatic mission performance gains from multiple customer and stakeholder perspectives. It is a key part of a process management approach for optimal performance that continually evaluates, adjusts or removes processes." -NAPA, 1995

It has been argued that government activities are often policy generators or oversight mechanisms that appear to add no value, yet cannot be eliminated. The concept of Re-engineering in the public sector is challenged on some of these premises. However, government only differs from the commercial sector because it has different kinds of controls and customers. It still utilizes a set of processes aimed at providing services and products to its customers.

It is evident that Government Process Re-engineering (GPR) is one of the essentials to bring about transparency in government working, reducing bureaucratic controls, increasing efficiency and productivity, reducing cost of service delivery. A GPR approach must rest upon a longer-term and more enlightened vision. This aims for a re-balancing of the 'front' and 'back' offices, as part of a gradual and deliberate policy to move resources and re-train staff from a more efficient and streamlined administration to direct citizen contact and service.

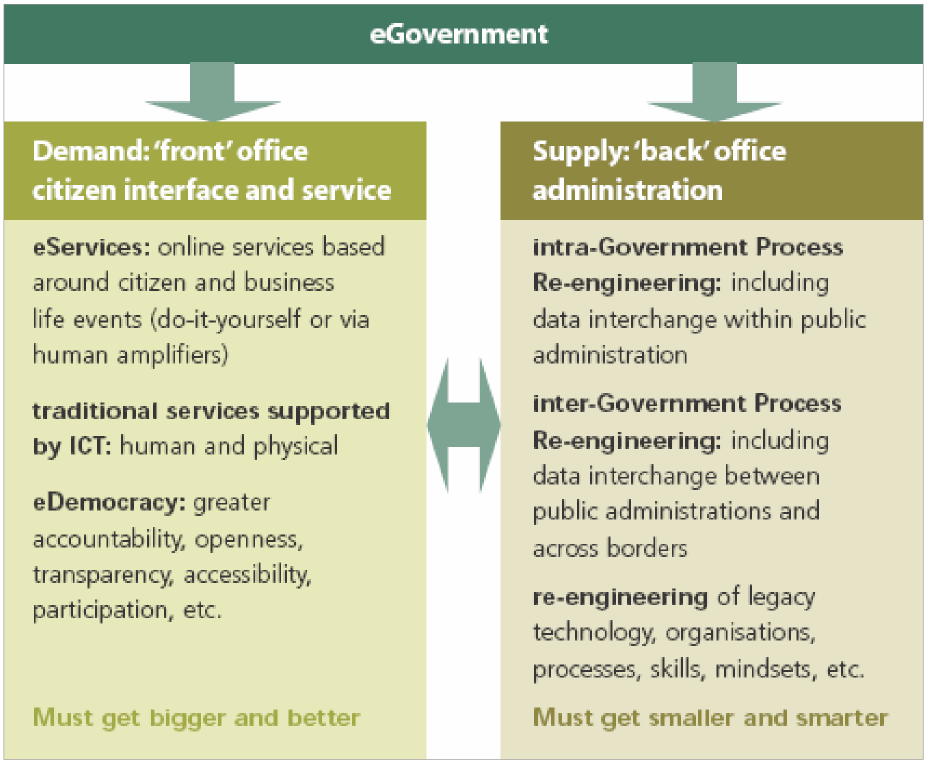

eGovernment
Demand: 'front' office citizen interface and service
eServices: online services based around citizen and business life events (do-it-yourself or via human amplifiers)
traditional services supported by ICT: human and physical
eDemocracy: greater accountability, openness, transparency, accessibility, participation, etc.
Must get bigger and better
Supply: 'back' office administration
intra-Government Process Re-engineering: including data interchange within public administration
inter-Government Process Re-engineering: including data interchange between public administrations and across borders
re-engineering of legacy technology, organisations, processes, skills, mindsets, etc.
Must get smaller and smarter

Figure 2: Re-balancing e-Government

ICT can support and enhance quality improvements to government services delivered in tradition, such as health, education and social care. It is important that the technology does not replace frontline staff when this would lead to a more impersonal, lower quality service, but rather directly supports such staff by improving the quality of the services they deliver and by making them more responsive to citizen needs. Rather than a technology-driven approach, it is important to let people do what people do best and the technology do what it does best.

Symptoms of Poor governance

Poor governance can be identified by signs of

- Air of mystification about procedures
- Long queues at delivery points
- Multiple visits to government offices
- Pillar-to-Post
- Outcome is in suspense
- Gatekeepers at every turn
- Poor quality of service
- Service is a mercy - not a right
- Too many intermediaries, shortcuts
- Extensive information exchange, data redundancy and re-keying
- Huge inventory, buffers and other assets
- Too many controls and checks, complexity, exceptions & special cases

7.4 Understanding Business Processes

Every government service is supported by a set of business processes, which provides approach and guidance to deliver the service. To understand Business Processes and Government Processes, consider the following definitions:

Process	A group of tasks / activities carried out to reach a (desired) outcome
Business Process	Any set of activities performed by a business that is • initiated by an event, • transforms information, materials or business commitments, • produces an output
Government Process	Any set of activities performed by a Government that is • initiated by an event, (e.g. Service Request, Event Trigger) • transforms information, materials or business commitments, • produces an output (delivery of Service to Citizen / Business of Government)

Government Processes are processes in the government domain. The process environment or a Business system is a collection of processes that take one or more inputs and create output that is of value to all stakeholders. Processes and not functions drive an organization. Processes are the key to satisfying customers and stakeholders.

Accordingly it should be the endeavour for the Government to improve its internal and citizen service delivery processes.

7.5 Understanding Service Quality

Service Quality is an important concept to be kept in mind while undertaking GPR initiatives. Service Quality comprises of the physical Product, the Time taken to deliver it, the Cost of getting the service, and Customer Experience or Service Delivery. A GPR exercise should identify the Service Quality Parameters associated with the service being re-engineered, and strive to improve those parameters.

To illustrate service quality, let us take the example of the Passport Issuance process. At first glance the only tangible product in Passport Issuance process is the physical passport itself. There are various parameters by which the quality of the physical product can be measured:

- Name & Photo are correct
- Personal information like sex, date of birth, address etc are correct
- The passport is stamped / signed and is valid
- Physical passport is as expected
- Not torn or damaged (Does not have pages missing / has correct number of pages)

But for a citizen, the Service Quality is dependent on a lot of other factors apart from the Physical product. These include a host of factors, including the following:

- **Time:** time taken for completion of service by the citizen/business, time taken for delivery of service by the Government
- **Cost:** Cost incurred in receiving the service by the citizen/business, cost incurred by the government in delivery of service
- **Complexity (illustrative):** Number of forms to be filled, amount of information to be provided, number of offices to be approached etc by the citizen/business
- **Transparency:** Knowledge on process for delivery of service, delivery timelines, status of service request to citizen and business
- **Citizen Experience:** Quality of interactions (courtesy, politeness, treatment) with the government during service delivery

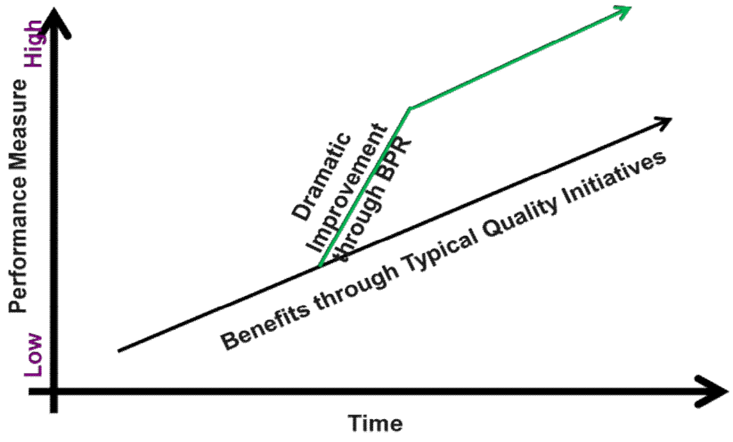
A holistic process improvement initiative should address all these Service Quality Parameters.

7.6 Business Process Re-engineering (BPR) and GPR

One of the widely accepted definitions of BPR is "BPR is fundamental rethinking and radical redesign of business processes to achieve dramatic improvements in critical, contemporary measures of performance, such as cost, quality, service and speed"

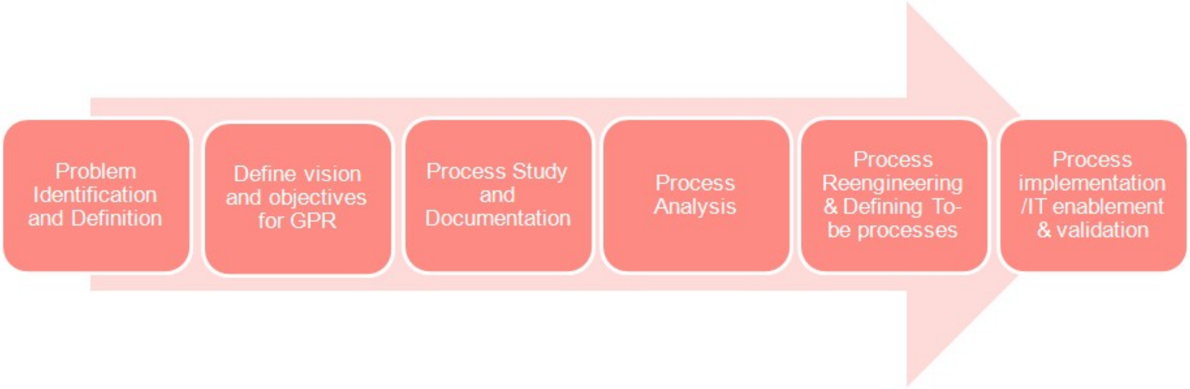
Government Process Re-engineering (GPR) has evolved from applying Business Process Re-engineering (BPR) concepts to Government Services. GPR may address all or some of the service quality attributes identified for the government service.

GPR enables governments to achieve dramatic improvement of performance and application of IT on reengineered processes will yield better results for stakeholders, as indicated in the graph below:


High
Performance Measure
Low
Dramatic Improvement through BPR
Benefits through Typical Quality Initiatives
Time

In order to leverage the full advantage of the GPR exercise, suitable IT enablement of the re-engineered processes should also be undertaken.

7.7 Steps involved in GPR


Problem Identification and Definition
Define vision and objectives for GPR
Process Study and Documentation
Process Analysis
Process Reengineering & Defining To-be processes
Process implementation /IT enablement & validation

The various stages in the GPR initiative are depicted above. The first step in the GPR process is the identification and statement of the problem in the current process scenario. This is followed by the definition of the vision and objectives of GPR. Before setting out on process re-engineering, the existing processes should be studied and documented. During this phase, data is also collected from the different processes, to understand the processes better and to obtain baseline metrics.

The processes thus documented are analyzed using various tools and methodologies, to identify improvement opportunities. This will include identification of value adding / non value adding activities, process complexity and process metrics.

During the re-engineering phase, the new processes are designed based on the process re-design drivers. This may involve rework, redesign, outsourcing or replacing of processes / sub processes. The new processes thus defined are implemented, with IT enablement (in most cases). The implementation phase may require changes in the legal framework governing the processes, and change management efforts to smoothen the roll-out.

Stage 1: Problem Identification and Definition
• Analysis of citizen grievances & complaints and pro-active Voice of Customer surveys • Analysis of issues raised • Identification of problem and defining unambiguous problem statements
Stage 2: Define vision and objectives for GPR
• Analyze services portfolio and undertake service prioritisation exercise • Define vision for GPR, from problems identified, service priority • Define measurable objectives for the GPR exercise
Stage 3: Process Study and Documentation
• Study process flow, actors, policies, process stages • Documenting as-is processes and creating Process Maps • Recording time and other data elements for each process step • Validation of process documentation from dept. • Identify and classify PIEs for the processes
Stage 4: Process Study and Documentation
• Root cause analysis of process issues and identification of root causes • Analyzing process efficiency - Value Adding and Non Value Adding steps • Analyzing process complexity - Data entry points, Hands off points etc • Definition of key metrics and arriving at baseline indicators (TAT, error rate etc)
Stage 5: Process Study and Documentation

- Elimination or automation of Non Value Adding / redundant activities
- Identification of solutions (re-engineered process)
- Evaluation and selection of best solution
- Definition of To-be processes based on the evaluation
- Finalization of To-be processes with department
- Setting of target KPIs

Stage 6: Process implementation l IT enablement & validation

- Implementation of re-engineered processes
- Implementation of IT system to handle re-engineered process flow
- Putting in place mechanisms to monitor KPIs and continuous improvement
- Change Management, Legal Framework changes etc

8. Change Management and Capacity Building in e-Governance

8.1 Change Management

The implementation of e-Governance programs brings along drastic changes in the routine functioning of day to day government. The delivery of Government services through the electronic media including EDI, Internet and other IT based technologies would necessitate procedural and legal changes in the decision and delivery making processes. It demands fundamental changes in Government decision management. There are changes in the processes, reporting structure, delegation of powers, administrative set-up, roles and responsibilities of the employees etc. The employees need to be delegated more authority. De-layering of the decision-making levels leads to Re-engineering and appropriate sizing of the decision-making machinery. All the changes in the system may not be welcomed by the stakeholders. These changes need not only be accepted by the government and citizens but also be accepted by various interests groups like employees unions. Under such circumstances bringing in a change will involve changing the mindsets of the people, and a complete Re-engineering process needs to be carried out for the same. Hence, implementation of e-Government programs necessitates change management. Change management is the methodology that integrates change and the ability to adapt into the organization. It is an organized, systematic application of the knowledge, tools, and resources of change that provides organizations with a key process to achieve their basic business strategy. This will involve training of the personnel at all levels, more so, at the lower rung of government management organizations.

e-Government implementation is complex for the following reasons:

- Inherent difficulties
  - Long implementation
  - Underestimation of effort
  - Benefits accrue in the end whereas effort required upfront
- Large number of stake holders
  - Who are the drivers: consultants, departments, ICT authority, partner
  - Degree of support from top management for investment and involvement in implementation
- Design issues
  - Processes consistent and transparent versus flexibility
  - Integrating with legacy systems
  - Technical performance
  - Privacy, security and standardization
- Management of change
  - Extent of process reform
  - Varying comfort level with IT/screens

The implementation of e-Government projects leads to a cultural shift for the government officials.

Traditional model	e-Governance model
A Civil Servant provides services mainly because of personal dedication. Jobs are secure. Only gross violation can really be "accounted" and handled. Promotions are linked to: • "Maturity" • New skills learned • Office Politics Good service cannot be accounted and therefore cannot be rewarded. New Technologies are threatening because of the new efficiencies.	Tracking quality of services enables to reward personal dedication. Promotions are linked to: • "Maturity" • New skills learned and applied • Personal capacity and creativity (Office Politics) New Technologies are opportunities thanks to the new revenue streams created

A reluctance or inability to manage change properly is often one of the key reasons for the failure of e-Governance projects. The discipline of change management identifies and addresses the human resources and organizational factors that can drive or obstruct change. Prof. Norman Archer has developed a simple but comprehensive methodology for analyzing change management. According to Dr. Archer: "an evolving Environment creates Change Drivers that impact the Organization". Management determines how to respond to these drivers. A Change Strategy is selected, along with Tools and Methodologies, for implementing the proposed organizational changes. It is critical to be able to Measure and Evaluate the impact of change on the organization, so an initial snapshot of the organization is taken. During and after implementing changes, the organizational impact must again be evaluated to determine whether it has been successful. Continuing adjustments may be required to tune the organization."

8.1.1 Change Management defined

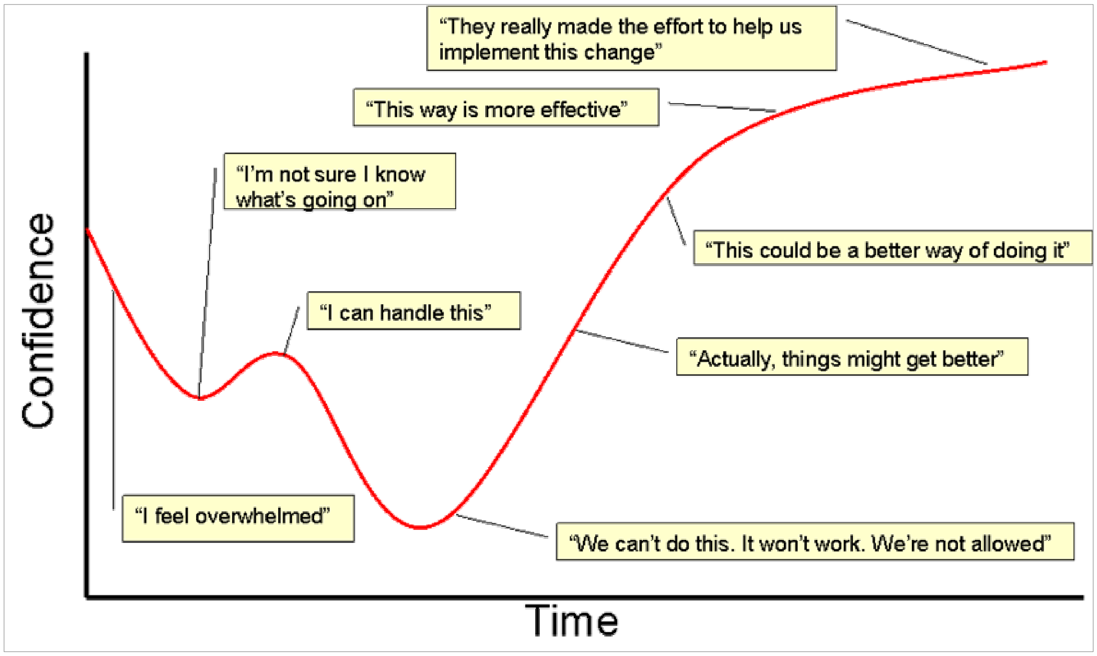
Change management is the methodology that integrates change and the ability to adapt into the organization. It is an organized, systematic application of the knowledge, tools, and resources of change that provides organizations with a key process to achieve their basic business strategy. Organizations manage change to:

- Identify patterns and structures of change in order to control them
- Predict issues and problems in each stage in order to accelerate change and minimize pain

An alternative definition: "Systematic identification and management of activities that enable an organization in transition from its current state to a desired future state. These activities include

communication, stakeholder engagement, transition management, training as well as evaluation of change readiness and change acceptance."
One of the most common starting points for applying change management is seen to be after the project has been conceptualized, designed and implementation has begun. Change management is often added after the project begins to experience problems. In reality, in most of the e-Government projects we see that change management processes are initiated only after the project implementation has started. This initiative again is mostly not taken with a holistic understanding of change management, and is taken as a reactive measure rather than pro-active measure. The present CMF may be used at any of the entry points of the project; however it is most effective to address the change management issues at a high level during the project feasibility and conceptualization study. Secondly, the change management process activities should be included as part of the project plan. Thirdly, it could [should?] be developed by an in house team having the required level of competency, and recommended to be facilitated by an external consultant team. Achieving successful change management with e-Governance requires you to use both individual and organizational change management approaches.

People reaction to change can be summarized in the following figure:



Key components of successful change management are:

- Leadership
- Focused and coherent strategy, including defined objectives and implementation plans
- Buy-In from stakeholders, which includes
  - Consultation
  - Incentives
  - Training
  - Monitoring and evaluation

8.1.2 "ADKAR" - a model for Change Management

ADKAR is a goal-oriented change management model that allows change management teams to focus their activities on specific business results. The model was initially used as a tool for determining if change management activities like communications and training were having the desired results during organizational change. The model has its origins in aligning traditional change management activities to a given result or goal.

The model was initially used as a tool for determining if change management activities like communications and training were able to obtain the desired results during organizational change. The model has its origins in aligning traditional change management activities to a given result or goal. As a project manager, the participants can use this model to identify gaps in their change management process and to provide effective coaching for their employees.

The ADKAR model can be used to:

- Diagnose employee resistance to change
- Help employees transition through the change process
- Create a successful action plan for personal and professional advancement during change
- Develop a change management plan for employees

The ADKAR model has the ability to identify why changes are not working and help you take the necessary steps to make the change successful. You will be able to break down the change into parts, understand where the change is failing and address that impact point

The ADKAR model works on the premises that change is a two dimensional process viz. Business dimension of change and People dimension of change. Successful change happens when both dimensions of change occur simultaneously.

8.1.3 Key Principles for Change Management design

The following factors must be considered while designing change management plan.

- Design compensatory benefits for real losses due to change for employees. Communicate positives and negatives honestly
- Ensure organization climate is right
  - Shared values with advocates of change
  - Participative design
  - Quality of work life, job satisfaction as explicit objectives
  - Training and education
- Ensure all stakeholders understand
  - Expected pay off
  - Role of stakeholders & others in terms of new tasks, skills, training
  - Counseling service, feedback on understanding
- Organization to manage change
  - Identify champions and legitimize role
  - Project team, command structure
- Identity obstacles to change in advance of implementation
  - Financial, technical, organizational, social, anti- champions
- Determine implementation strategy staged/phased, incentive structure

Organizational dimension of change

The business dimension of change includes the typical project elements.

- Business need or opportunity is identified.
- Project is defined (scope and objectives).
- Business solution is designed (new processes, systems and organizational structure).

- New processes and systems are developed.
- Solution is implemented into the organization.

These are the standard elements of a business change that managers feel most comfortable managing

People dimension of change

Research shows that problems with the people dimension of change are the most commonly cited reasons for project failures. In a study with 248 companies, effective change management with employees was listed as one of the top-three overall success factors for the project. Helping managers be effective sponsors of change was considered the most critical success factor overall.

Effective management of the people dimension of change requires managing five key goals that form the basis of the ADKAR model:

- Awareness of the need to change
- Desire to participate and support the change
- Knowledge of how to change (and what the change looks like)
- Ability to implement the change on a day-to-day basis
- Reinforcement to keep the change in place

8.1.4 Communication in Change Management

There are five key principles of Effective Communication:

Principle No.1: Organizational Change cannot occur without communication.

Principle No.2: Communication is not a single step or component of a change process - it must occur in parallel, fully integrated with the change process.

Principle No.3: Communication strategic planning entails more than selecting ingredients or tactics according to a cookbook or recipe.

Principle No.4: Communication is not something done to a target audience, like turning on a fire hose of words. Effective communication is a two-way process, focused on dialog.

Principle No.5: Communication professionals apply the rigorous planning process, including assessing stakeholder needs, creating and coaching message delivery, and building feedback loops.

Some of the errors in change communication are:

- No clear identification of key stakeholders/audiences
- Failure to listen to stakeholders (attitudes, concerns, information needs, suggestions)
- Insufficient faith in stakeholders' ability to handle "bad news"
- Lack of candor
- Concentration on the "what" at the expense of the "why"
- Failure to analyze communication processes/channels internally and externally (what works and what does not)
- Over-reliance on established media
- No high-level, strategic accountability for communication
- No clear spokesperson/spokespeople

- Failure to define consistent "major messages" for all stakeholders
- Focus only on initial announcement and end results - rather than on continuous information sharing and reinforcement
- Lack of predictability (communication frequency and channels)
- Belief that confidential information will stay secret

8.1.5 Key Reasons for Failures in Change Initiatives

In-spite of all planning, sometimes a change initiative may fail. The reasons for failure may be within control of the Project leadership team or beyond its control. However, being aware of at least potential causes of failure, which are within the control, is a pre-requisite for successful change management. Following are some of the reasons for failure of a project:

- **No prioritization:** Every activity is given equal importance and priority. All or most of the activities are taken up simultaneously, making the change process complex and unmanageable.
- **Voice of customer is absent:** The objectives of the change do not take into account the requirements of the customers. Customers are either not consulted or their needs are ignored or their requirements are misunderstood.
- **Employees are not involved:** Little or no involvement of employees in the implementation of the project finally becomes a major impediment to the change initiative.
- **Benefits at individual level are not demonstrated:** The project may aim to provide signification benefits at Organizational level. However, for the individuals involved (employees, citizens, etc.), there may not be any clearly perceivable benefits. Such a situation creates resistance to change, finally leading to project failure.
- **No urgency is created for Change:** This aspect is often overlooked. People generally tend to remain in the 'As-Is' situation and resist any attempt to change. In case of ILIS, the efforts to create 'urgency' for 'change' has to be directly proportionate to the complexity of the Project.
- **Continuity of team not ensured:** Many e-Governance projects suffer due to changes in the project leadership and management teams. When new members come on board, there is whole lot of things to be learnt about the project activities, risks, etc. This takes its own time and slows down the project progress. Lack of continuity in project team also deprives the project of the key benefits that come with experience.

8.2 Overview of Approach for Change Management

This section discusses overview of approach for managing the change in e-Governance projects implementation. Change management is the process, tools and techniques to manage the people-side of business change to achieve the required business / organizational outcome, and to realize that business change effectively within the social infrastructure of the workplace. The Change Management in e-Governance projects implementations focuses along three key dimensions. These are:

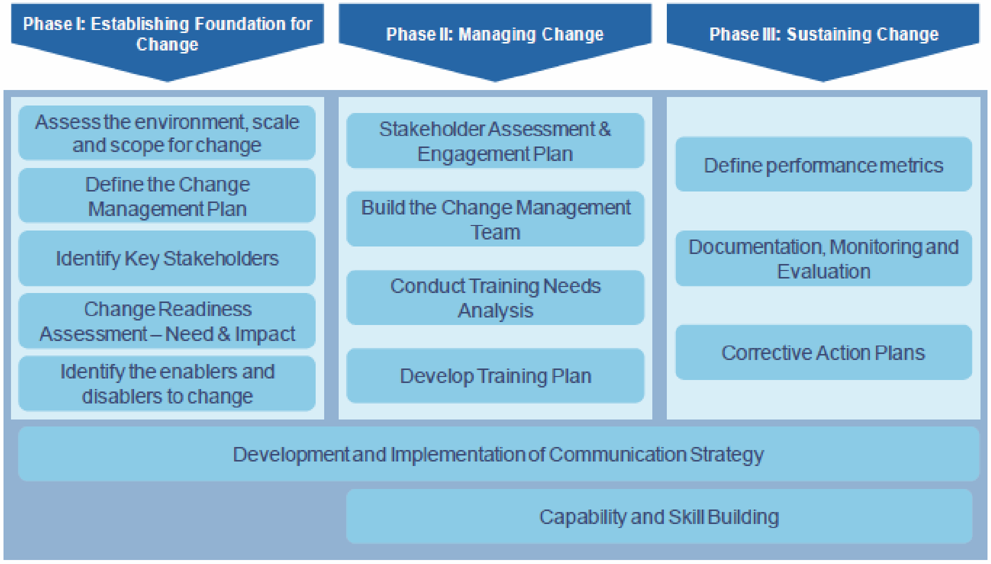
Essential elements of Change Management

Stakeholder Management	Make sure all stakeholders are identified, relationships are managed; stakeholders get information about progress, program needs, and benefits tracking, their feedback is received and incorporated in the program
Communication Management	Provide planned communication throughout the organization and execute this along effective means and channels. Make sure that communication reaches the target audience in time and provides just enough information for that audience so that they are informed on and excited about the change and effectively implement it
Training	Provide training materials, trainers and logistics; ensure the target audiences are trained in the new ways of working (including data,

processes, systems/tools and governance) just in time and just enough.

Based on these key elements, the diagram presents overview of approach for managing people change in e-Governance projects implementation and later paragraphs summarizes key activities performed in each phase of approach.

Approach for Change Management


Phase I: Establishing Foundation for Change
Phase II: Managing Change
Phase III: Sustaining Change
Assess the environment, scale and scope for change
Define the Change Management Plan
Identify Key Stakeholders
Change Readiness Assessment – Need & Impact
Identify the enablers and disablers to change
Stakeholder Assessment & Engagement Plan
Build the Change Management Team
Conduct Training Needs Analysis
Develop Training Plan
Define performance metrics
Documentation, Monitoring and Evaluation
Corrective Action Plans
Development and Implementation of Communication Strategy
Capability and Skill Building

Stakeholder Management, Communication and Capability Building (Training) cut across the different phases of the Change Management Framework, which clearly indicates the importance of these activities in the overall Change management initiative. Following lists key activities at each phase of the change management approach.

Phase I: Establishing Foundation for Change - Key Activities

- Assessing the Scale of change in terms of number of affected entities, users, geographical spread, etc.
- Assessing the scope in terms of policy, process, system and structure
- Assessing the existing environment to understand 'Change Readiness' and 'Culture' Assessments
- Preparing a Change Management Plan
- Identifying the key stakeholders, in terms of people impacted and those capable of influencing the outcomes of the change initiatives
- Identifying the key enablers and disablers of Change

Phase II: Managing Change - Key Activities

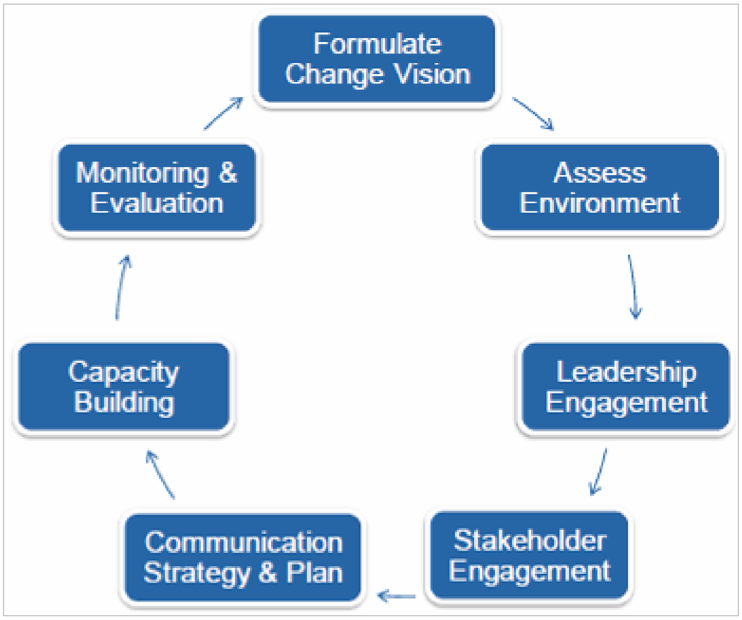
- Assessing the stakeholders for understanding their power, influence, impact and support in the project
- Mapping of various stakeholders and stakeholder groups
- Building the Change Management Team to make change 'happen'
- Defining the roles and responsibilities of the members of the Change Team
- Conducting Training Needs Analysis to understand the training objectives
- Prepare the Training Plan for addressing the training needs

Phase III: Sustaining Change - Key Activities

- Identifying the performance metrics for measuring the success of 'Change' and cascading the same to the stakeholders
- Monitoring and evaluating the metrics to measure the change outcome and incorporate necessary modifications
- Developing a repository / knowledgebase for documentation of the 'Change'

8.3 Guiding principles for Change Planning

A Change Management Plan defines the various phases, related activities, tools and mechanisms for evaluating and tracking the changes and the related deliverables encompassing a Change Management initiative. Following are the guiding principles for change planning.



Guiding Principles	
Guiding Principle 1: Formulate Change Vision	• Creating a compelling vision for change is key to implementation of any Change Management initiative. • Vision acts as a bridge between the current state and the desired future state. • Vision should be defined and articulated at the onset of a Change • Management initiative.
Guiding Principle 2: Assess Environment for Change	• Assess the environmental variables influencing the change process viz. legal, political, social • Assess government's / department's history, readiness and capacity to change • This Assessment should be carried out in the initial stages of planning, as it will help in identifying risks and developing a plan to mitigate them

Guiding Principles	
Guiding Principle 3: Leadership Engagement	• Leadership needs to create, drive and support the change agenda. • Leaders must understand the dynamics of change management and need to apply the principles that make change effective • Leadership engagement to visibly lead the change, set the tone for change, and reinforce the government's commitment to the interventions must be outlined at the planning stage
Guiding Principle 4: Stakeholder Engagement	• Identify and engage the key stakeholders at the beginning to minimize the resistance from change and create buy-ins • Engage and collaborate with stakeholders affected by the change as much as possible
Guiding Principle 5: Communication Strategy and Plan	• A targeted approach to developing a communication strategy is important in e-Governance projects • Communication strategy should be developed during the Planning phase of change and needs to be revisited and refined throughout the change cycle • Communication needs to be assessed by looking at the why, what, how, and when of communicating • Change program should aim at creating awareness, and gaining support, involvement and commitment
Guiding Principle 6: Capacity Building	• Training of the personnel at all levels is imperative to build capacity and sustain change in e-Governance projects. • Identifying key skills required to drive and implement the change initiative must begin at the planning stage. • The training plan must be charted out for identified groups and targeted training must be conducted. • Few leadership training might be required at the onset to equip the leaders with the necessary skills to drive the change
Guiding Principle 7: Monitoring and Evaluation	• Define metrics/system to measure progress of the change initiative - how far have we got, how far do we still need to go? • Monitoring techniques need to be designed by the project team and cascaded to the key stakeholders.

8.4 General Tools in Change Management

The table below discusses general tools in change management planning and execution

General Tools	
Change Readiness Survey	• Measures the organizational readiness to change, and • Determines the levels of understanding, acceptance and commitment likely to effect the success of the planned change **An assessment should answer:** • How will people respond to change? • To what extent will they "own" the change? • Where might there be pockets of resistance? • What are the systemic or cultural barriers to effective change implementation? • What strategies and methods should be deployed to minimize resistance, reduce barriers and promote ownership?

General Tools	
Change Management Workshops	• Meetings emphasizing on exchange of information among a usually small number of participants through hands-on exercises • An effective tool to facilitate discussions involving change leaders • Decision makers and their supporting teams in the right mix • Creating an effective agenda for workshop including Cleary defined objectives, Flow of the activities in the workshop, Communicating expectations to the participants and Guidelines for the moderator / facilitator
Large Scale Interactive Process (LSIP)	• LSIP works on the Philosophy that "If the dissatisfaction of the people is understood, then people are propelled to look at the vision of the organization. The creative tension between the dissatisfaction and the future vision helps people in taking the first steps towards change." • LSIP can be used as an effective tool while communicating the change vision to a large group of stakeholders in relatively short period of time
Structured Interviews	• A structured interview is an interview format where a defined set of questions are asked from various individuals • The tool can be used to conduct perception and engagement surveys in a Change Program **Principles of designing structured interviews:** • Questions are presented with exactly the same order • The choice of answers to the questions is fixed (close-ended) in advance • Open-ended questions can also be included but within a defined scope • An interview schedule which lists the wording and sequencing of questions
Focus Group Discussions	• Focus group methodology is one of several tools to generate valid information important to the advancement of change programs across organizations through a group interview technique. **Principles for conducting focus group discussions:** • 10-12 participants from a similar group • Participants are asked to provide insights on the topic and there is no fixed response to a particular question - • People may tell personal stories, revisit an earlier question, disagree, contradict themselves, and interrupt. • Facilitator must balance the needs of participants to 'have their say' against the need to stay focused. • Reporting and analysis is done in words not numbers

General Tools	
Appreciative Inquiry	• Appreciative enquiry is a useful and effective approach used for thinking, seeing, and acting for powerful change in organizations. • It works on the assumption that whatever you want more of, already exists in all the organizations and this process allows change leaders, drivers to discover that. **Approach** • There are a variety of approaches to implementing Appreciative Inquiry: o Mass-mobilized interviews o A large gathering of stakeholders o Group discussions • All these approaches involve bringing large, diverse groups of people together to: o Visualize the future in a positive way o Study and build upon the best in the organization / system. • Questions: o Questions are designed to encourage people to tell stories from their own experience of what works in the organization / system o Questions often revolve around what people enjoy about their aspirations for the Future • Participants: o The process begins with a core group setting the focus of the Inquiry, and developing and testing the appreciative questions. o Then the questions are shared with a larger group of people. • Time Requirements: o The interview questions can be developed, tested and analyzed in a few hours or in a workshop. o Data from the interviews can be looked at and turned into information by a few people in the design team o Everyone can then decide collectively how to best go forward.

General Tools	
Identifying Key Stakeholders	• Identifying the key stakeholders early in any e-Governance project is important. • Stakeholders are defined as individuals and groups - internal or external to an organization - who are impacted by and capable of influencing the outcomes of change initiatives. • Stakeholders are identified by scanning the ecosystem of the e-Governance projects. • When identifying key stakeholders, consideration should be given to: o **Location of the stakeholder:** Where are the key stakeholders located in the organization's broad structure. Government headquarters, state-union level. o **Role in the decision-making process:** What role do these stakeholders have in decision making. Identify People those influence decisions in a particular situation or regarding a particular issue, i.e., Those that are most active in making decisions, taking actions and communicating and those who will take decisions on the transformation program or whose decision making capacity could impact the success of the transformation program. o **Position:** Some stakeholders may be identified as important in particular situations or for particular issue because of the roles they play and the positions of influence or power they hold. e-Governance policies are framed at the highest levels of Government involving politicians and bureaucrats. o **Membership:** Affiliation and membership of a professional association or special interest group may be important because they can have influence/power in a situation e.g., industry bodies or trade unions.

8.5 Change Management

8.5.1 Understanding Environment, scale and scope for change

We discussed in the previous sessions, various environment variables, which exert an impact upon implementation of e-Governance projects. These variables are categorized as Social, Political, Legal and Economic variables. For minimizing the impact and resistance from people, it is vital to understand the scope of change led by the e-Governance projects. Few questions that need to be answered to understand the scope and scale of change of the e-Governance Projects:

- To what extent will there be changes in the way the Government departments operate, is structured, or work?
- Will the change require a shift in mindsets and behaviors?
- How many elements (i.e., people, process, structure, and strategy) will be impacted?
- To what extent will the Government organization (i.e., departments, workgroups, the number of people, functions, and locations) be affected?
- Who are the key stakeholders and target audiences in the overall change program?
- How much emotional impact will the change have?

a) Understanding Scale of Change in an e-Governance Project

Scale of the 'change' refers to entities affected by the change, number of users geographical spread. Scale of the 'change' can be understood through leadership discussions in the Government and with other key stakeholders.

Scale of change (Indicative factors)

- Number of employees / stakeholders who will be impacted due to implementation of the project
- Units across which the proposed system will percolate

b) Understanding Scope of Change in an e-Governance Project

It requires adequate focus and experience to manage peoples' apprehensions, aspirations and capacities during e-Governance projects cutting across policy, process, system and structural elements and that would likely involve physical relocation in addition to the acquisition of new skills and a change in roles for the workforce. The scope of change in e-Government projects in general is along policies, processes, systems and structural changes. For effectively managing the people change, it is critical to gain good understanding of what is the scope of change along these dimensions. Based on the scope and scale of change, necessary change management planning can be performed.

8.5.2 Approach for assessing the environment, scale and scope for change

Assessing the environment for change at the onset of any change management exercise is key to the success. Tools such as Change Readiness Assessment and Culture assessments can be used for diagnosis. An understanding of the Change Situation can be gained through an enquiry into 5 key areas: (i) Context, (ii) Complexity, (iii) Consequence, (iv) Culture and (v) Capability.

a) Context for change

Context explores the nature and driving forces behind the change initiative. E.g. The purpose of most of the e-Governance initiatives is to reform the way Government manages and shares information with external and internal clients. Specifically, to harness ICTs (such as Wide Area Networks, the Internet, and mobile computing) to transform relations with citizens, businesses and amongst various arms of Government.

- **Predictability:** It is important to understand, How certain or clear are the outcomes and benefits resulting from an e-Governance project? What is the vision of Government and the Leadership team from the project?
- **Urgency:** How critical or time-constrained is the project and the need to bring in the desired change?
- **Inherent risk:** How serious are the consequences for the organization if the change fails?

b) Complexity

Identifying & Understanding the key variables contributing to the complexity of e-Governance projects at the onset can be used as a critical guideline while designing the change approach & strategy.

- Examine the complexity of the problem and predictability of the solutions.
- Also key here is the complexity of the structure of the Government entity and its interdependencies and interactions with various bodies and its possible impact on successful change implementation.
- Finally, time and space constraints need to be understood.

c) Consequence

Understanding the levels of resistance is critical for an e-Governance project to create buy-in from all the stakeholders at a later stage.

- Review of the likely levels of resistance to the proposed changes, on a role by role and unit by unit basis
- Review of potential areas of resistance and also the organizational politics especially amongst the leadership of the organization

- Understanding the inherent consequences to the individual/organization of either complying or not complying with the proposed changes.
- Understanding the extent to which the delivery of the benefits of the program is dependent on any particular change approach.

d) Culture

Cultural barriers pose the biggest challenge in installing a new system. They exist at employee level, officers' level and political level. The need is to create a rich and adaptable culture that encourages values which opens up the bureaucratic structure of the Government organizations. Culture looks at norms of behavior in the organisation, including a review of how change has/has not been implemented successfully in the past.

- Are people focused on detail or the big picture?
- Is there a power and control culture or a culture of empowerment?
- Do people focus more on the task or on the people?
- In case the change effort is on a national scale, assessment of regional cultural differences is essential

e) Capability

Mostly e-Governance projects start on the assumption that capability is available within the organization to deliver such programs. However, an unrealistic guesstimate can derail the program, hence, a systematic approach to understanding current capabilities is important to design realistic change management strategy. Understand the capabilities (current and required) to both implement the change and operate sustainably in the new environment.

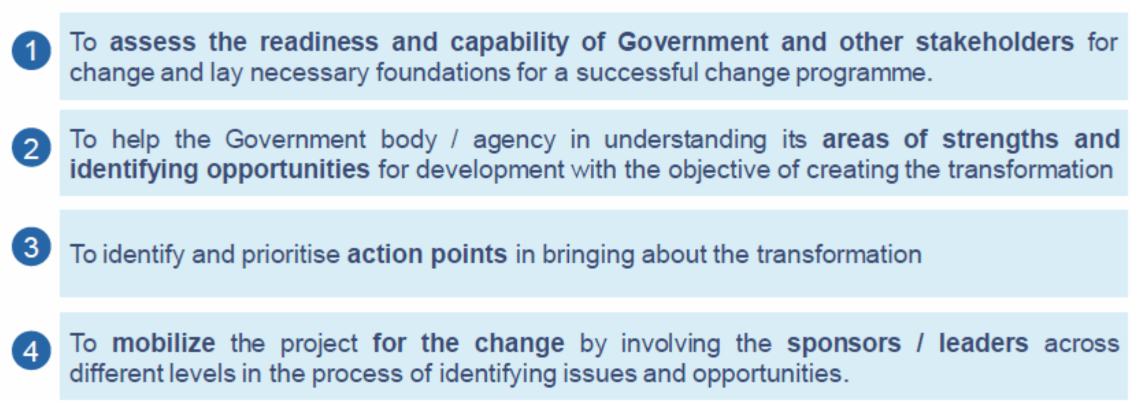
- Assessing the skills and capabilities of the organizational Leadership to drive the change process
- Look at available resources and understand other change efforts currently underway in the Government agency / body.
- The level of commitment of both leaders and front-line staff should also be explored.

8.5.3 Identifying enablers and disablers to change

Identification of enablers and disablers is a an essential element in people change management, based on which effective stakeholder engagement and management strategy can be developed to leverage enablers and to address disablers for change. In identifying enablers and disablers for change, change readiness assessment plays a crucial role. Change Readiness Assessment is a systematic technique which provides data on organization’s capability to change and the change management 'hot spots' or risks that will inform the change strategy/plan. The assessment usually involves a combination of survey and focus group workshops with the following objectives:

- To understand how well the organization has delivered change programs in the past
- To understand current level of confidence in delivering future change
- To understand the gap between current capability and that required going forward
- To define and agree the change management actions to close the gap

It is a stakeholder engagement activity, and entails consultation and involvement of key stakeholders and members of the front-line. The key objectives of the Change readiness assessment are:

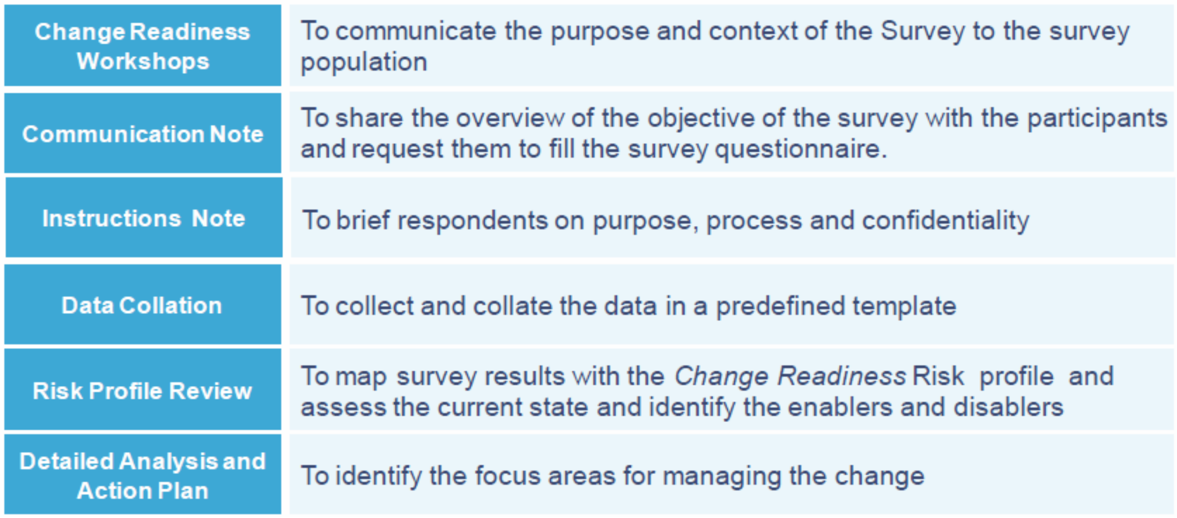


1. To **assess the readiness and capability of Government and other stakeholders** for change and lay necessary foundations for a successful change programme.
2. To help the Government body / agency in understanding its **areas of strengths and identifying opportunities** for development with the objective of creating the transformation
3. To identify and prioritise **action points** in bringing about the transformation
4. To **mobilize** the project **for the change** by involving the **sponsors / leaders** across different levels in the process of identifying issues and opportunities.

Change Readiness Assessment program will include following activities:

- Prepare sampling plan to cover stakeholders from various groups
- Develop a Change Readiness Assessment Questionnaire based on the identified change themes/levers
- Prepare administration plan and deploy various mechanisms such as workshops, e-mail, online, telephonic discussion, one-to-one meetings etc to collect the inputs of various workgroups.
- Collect and analyze the data.

Following lists key elements in change readiness assessments followed by overview of each of element.



Change Readiness Workshops	To communicate the purpose and context of the Survey to the survey population
Communication Note	To share the overview of the objective of the survey with the participants and request them to fill the survey questionnaire.
Instructions Note	To brief respondents on purpose, process and confidentiality
Data Collation	To collect and collate the data in a predefined template
Risk Profile Review	To map survey results with the *Change Readiness* Risk profile and assess the current state and identify the enablers and disablers
Detailed Analysis and Action Plan	To identify the focus areas for managing the change

a) Change Readiness Workshops

Change readiness workshops are used to communicate the purpose and context of the Survey to the survey population. Following are some key insights into change readiness workshops.

- Change readiness workshops aim at sensitizing the employees and other key stakeholders to the change process and gather their perception.
- It is an effective tool for gathering Top Management perspective and identifying key enablers and disablers to change
- Identification of change Levers which are imperative for achieving technological change in the organization

- Provide insights on e-Governance

b) Communication Note

Communications note is aimed at sharing the overview of the objective of the survey with the participants and request them to fill the survey questionnaire. Communication note includes:

- Message from the leadership
- Provide basic information around the concept and scope of the e-Governance initiative
- Objective of the Change Readiness assessment survey
- Explain how data will be used
- Assure anonymity and confidentiality
- Outline how the questionnaire needs to be filled

c) Instructions Note

Instructions note is aimed at briefing respondents on purpose, process and confidentiality including the guidelines for filling the questionnaire. This includes:

- Provide candid and honest response to the statements in the questionnaire.
- Give first reaction and not spend too much time thinking of each question
- Fill in the mandatory sections viz. Designation, rank etc. Name is optional anonymity is guaranteed.
- Provide the opinion in the context of your department and your role in the concerned unit / section.
- Fill in the circle in the scale that corresponds to the degree of your agreements to the statements

d) Data Collation

To collect and collate the data in a predefined template. Data collection can be done using a standardized template / questionnaire and can be gathered through workshops, online administration depending upon the culture of the Government department and technology availability.

e) Risk Profile Review

Risk Profile Review is used to map survey results with the Change Readiness Risk profile and assess the current state and identify the enablers and disablers. Diagram below presents a sample risk profile. The numbers in the diagram represent priority order for managing change based on the survey score.

f) Analysis of results to identify the enablers and disablers

Survey responses are analyzed by mapping them on the risk profile i.e. high, medium and low and the analysis is done from various perspectives to capture the gaps, issues and resistance among various employee groups.

The objective of overall change readiness assessment is to identify the change enablers and disablers. Following lists sample change enablers and disablers.

Change Enablers	Change Disablers

• A compelling change vision has been created and cascaded throughout the organization. • The leadership at all levels, drives continuous communication to explain change purpose • Active change management techniques are engaged to generate understanding and involvement among employees. • There is an established structured plan in line with the change vision. • Performance measures are established at organizational, functional and operational level.	• Stakeholders have fragmented understanding of the long term objectives of the technological change. • There is lack of structured plan, strategy and direction to guide organization response to change. • There is lack of commitment to the current change programs. • There is no visible leadership at functional / organizational level which drives change • Little or no formal communication outside the change program team.

Based on the identification of risk areas and analysis of the data course of action is determined for each dimension. E.g. Change Strategy, Change Commitment, Change Leadership, Communication Capability and Organizational Culture.

8.5.4 Building change team

For successful implementation of e-Governance projects, the project stakeholders need to be engaged and involved right from the beginning of the project. Following lists some key reasons for stakeholder engagement and involvement throughout project Lifecycle:

- Determine the level and type of stakeholder activities required to inform, involve and engage with them.
- Invest the appropriate resources to engage with stakeholders who are 'critical'
- Make sure that the Stakeholders are aware of their roles and responsibilities in ensuring success e.g., ICT implementation, the identification and acceptance of the responsibility for owning and managing the day-to-day aspects of the system and the new ways of working
- Minimize resistance to the program through stakeholder engagement strategies and prevent the program from being derailed
- Build a vision & hunger for success for the program & generate enthusiasm for the change
- Identify the extended audience for project communications and the project-related information that each stakeholder or stakeholder group should receive and with what frequency;
- Ensure that all of the project dependencies have been identified and their impact understood
- Stakeholder Engagement in an e-Governance program is an ongoing activity
- Stakeholders may move up and down the map as the project progresses so this work should be revisited on a regular basis
- List of stakeholders may also change throughout the Lifecycle of the project

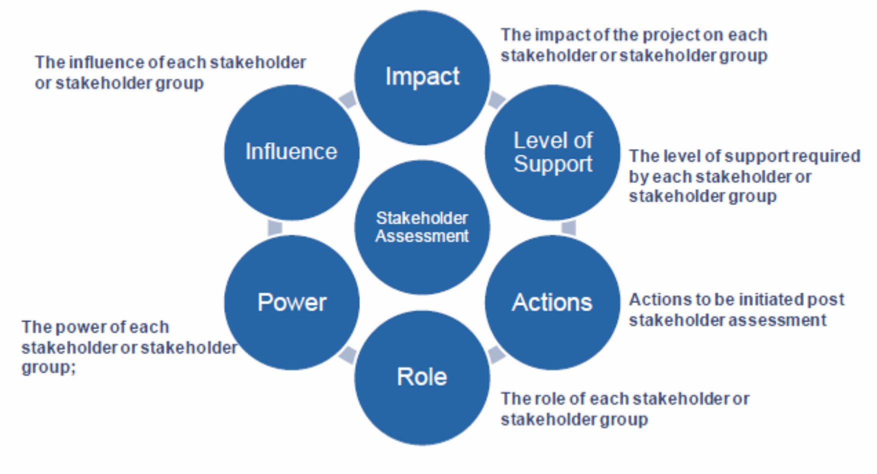
For effective stakeholder engagement and involvement, it requires an internal team, apart from the team of consultant, to support and drive the stakeholder engagement. This team can be referred as the change team.

A Change Team identified for change management plays a crucial role in implementation of change, communicating the change and leading the change at various levels of the organization. Hence, selection and formation of a change team will determine the success and outcome of the change management. For identifying the change team, it is important to understand the target stakeholder groups, who need to be managed, communicated and trained throughout the engagement. Some of the key stakeholders in an e-Governance Project are:

- Individuals such as Secretaries, Head of Ministries, Heads of Directorates;

- Project sponsor, Project manager, Heads of budgeting and spending units in pilot Ministries; Business process owners; Funding Agencies
- Consultants, Vendor/ Intermediaries
- Divisions, departments or units, employees, user groups, legal entities, or location / geography (e.g., headquarters, plant, location, state, country), citizens

All these stakeholders can perceive the same project in different ways depending upon their expectations.
Stakeholder assessment defines the power, influence, impact on the project and support required from the stakeholders and stakeholder groups.
Following parameters are used with a rating scale to assess and map various stakeholder groups in organization.



Impact
The impact of the project on each stakeholder or stakeholder group
The influence of each stakeholder or stakeholder group
Influence
Level of Support
The level of support required by each stakeholder or stakeholder group
Stakeholder Assessment
Power
Actions
Actions to be initiated post stakeholder assessment
The power of each stakeholder or stakeholder group;
Role
The role of each stakeholder or stakeholder group

Build a Change Champion network

Evolution of e-Governance change champions is essential and critical for handholding the e-Governance effort in the initial period. They act as catalysts to accelerate acceptance process among users and to ensure rapid deployment internally, by

- Facilitating acceptance
- Motivating the front end service people
- Create an awareness and curiosity among the users by explaining the benefits

Change Champions can extend the scope of communications for the Programme. They provide another avenue to communicate with the business and gather valuable feedback from the business. An ideal change agent in the e-Governance implementation would be:

- A computer savvy person
- Who has power and authority in governmental system
- High credibility among service department and user communities. Building a Change Champion Network that can make change happen:
- Find the right people: The stakeholders analysis will provide inputs for identifying the change champions for the program
- Create Trust: To facilitate teamwork among the Change Champions identified
- Develop a common goal: A common understanding of goals will help the team move in one direction

The change champions organization:

- Understand and agree with the need to change
- Have credibility and respect within the stakeholders (external / internal)
- Have a sense of urgency about the change
- Are good communicators and motivators

- Have a good understanding of the organization and it's culture
- Have great listening skills
- Are enthusiastic to represent the change within the organization
- Are approachable and accessible.

Four key characteristics seem to be essential towards building effective change champions network. They are:

- Position Power: Are enough key influential players on board?
- Expertise: Are the various points of view, relevant to the task at hand represented in the network?
- Credibility: Does the network have enough people with good reputation in the organization / amongst stakeholders?
- Leadership: Does the network include enough proven leaders to be able to drive the change process?

Roles of a Change Champion

- Change Leaders - Champions the Change vision, Guides, Removes barriers
- Cheerleaders - Educators, facilitators, Play supportive role, Removes barriers
- Program Manager - Plan change process with sponsors, Ensure project team has necessary skills, training
- Functional Change Experts - Deep subject matter expertise, Coach
- Change conceptualizers - Facilitate meetings, build creative environment, Integrate ideas into change design

8.5.5 Develop Change Management Activities

Development of Change Management Activities/Plan focuses on building the framework for the change implementation, where resources, roles and responsibilities are documented, schedules are developed based on timeframes and deadlines, and training requirements are identified. Development of change management activities refer to identifying various activities which are needed for helping/supporting each stakeholder group for addressing the risks/issues identified in during the change readiness assessment survey. From this analysis, the approach for addressing these issues and managing the change for project stakeholders should be developed including areas such as:

- A phased or staged approach to implementation of proposed e-Governance initiative from the people perspective as it will involve re-alignment of roles and re-training of the skills both functionally and behaviorally.
- Defining the associated measurement criteria for the items that will constitute the successful migration and its acceptance

Once the approach for implementation is defined, the various components of the current and planned future environments should be analyzed to determine which specific activities/actions are required to develop a successful migration strategy. For creating a lasting change effect for the project implementation, departments need to review and translate following key aspects into change activities. These would involve:

- New Roles - Creating and strategizing communication on the aspect of changed and value added roles in line with the requirements of project.
- Changes in Roles/positions/retrenchment/relocation - Creating and strategizing communication on the aspect of redeployment, retrenchment of employees and approach for managing the response/reaction from the employees.
- Identifying New Competencies - As current skills may not be sufficient for future

organization identifying and then communicating the need to raise skills levels across functions including sensitization to risk management becomes a key change management activity.

- Facilitating Cultural Change - Creating an advocacy culture across levels becomes critical in implementation of change programs as word of mouth and informal communication is key to successful implementation. We would look at the audience and create mechanisms for change management activities around the requirements from the aspect of cultural acceptance of change.
- Communication - It is imperative that communication is a dimension inter-woven in any change program and needs to intersperse and permeate through the entire change process.
- Recommending transparent HR and related sub-systems - Designing and creating systems helping people to understand their own skill gaps and therefore being able to take actions is key to generate buy in into the change program. Activities to align individual and organizational requirement are key to our change management approach, as we synthesize processes and systems to delineate non-transparency.

As departments go about designing activities around the above-mentioned requirements on the change management imperatives, the focus area should be two fold to lead the desired change:

- Inspirational to energize people, align people across levels and to chart a collectively accepted plan of action till the "go-live" phase.
- Operational to Re-engineer and design key business processes with the aim of achieving project objectives, to Implement Re-engineered processes and to Design suitable structure, systems and processes to sustain the change

Based on the above, departments need to identify the stakeholder wise Engagement and Change Actions/Activities based on the impact assessed for the target stakeholder groups and priority and sequencing of each change activity identified for the project. These change management activities are likely to consider, for example, change strategy, engagement and communications, change leadership, capability development, clarity and understanding of the case for change and vision.

For each change action/activity, department need to identify the stakeholder responsible for undertaking the activity and the approach for monitoring the change activity plan and effectiveness of change activities implemented during the project implementation. Following outlines key illustrative activities for Change Management.

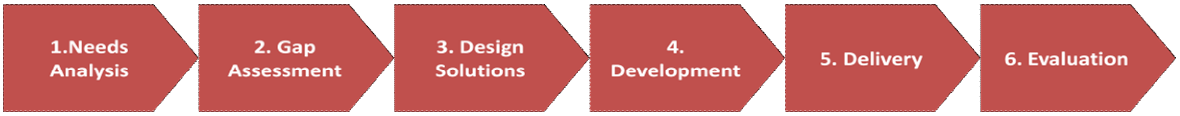
Activity	Description
Align Leadership	Facilitate the alignment of leadership relating to the support and advocacy of the overall change vision. This alignment shall be completed during the design phase to ensure leadership's support during the
Establish Change Program Governance	Leadership should be aware of the change program's progress, successes and risks so that impending decisions are made with an appropriate level of knowledge. The right teams must also be mobilized and empowered to make decisions regarding the change. Change program governance ensures that the right people are making the best decisions possible.
Select Appropriate Methods to Build Commitment	The purpose of this task is to develop a comprehensive understanding of communication in the organization and to determine and plan the best communication methods for the situation/message based on stakeholder needs and preferences. These comprehensive, detailed plans educate, involve and inform stakeholders, helping to build acceptance and buy-in throughout the transition.

Assess Training Needs and Curriculum Planning	The purpose of this task is to confirm the impact of the change initiative on all stakeholders, assess the training need, and design appropriate Curriculum / training plans that will enable end-users to successfully perform their jobs in the new environment. The training and curriculum plan should addresses policy, process, and system/tool training as well as other change management and leadership training as needed.
Involve & Educate Sponsors and Change Agents	It is important for all sponsors and change agents to be knowledgeable about the change program, as they will be responsible for addressing issues and concerns that may arise throughout the course of the change initiative. This task involves conducting training programs and workshops to educate all sponsors, change agents and the appropriate stakeholders.
Align Organization & Culture	Where appropriate, detailed designs and plans for recommended changes will be produced to support the change effort and integrate with existing organization design and cultural alignment activities.

8.6 Training in e-Governance Projects

Implementation of e-Governance projects may require significant changes to the current capabilities and skill sets of the employees in the organization and it is imperative to address the gaps between the required and current capabilities and skill sets of employees at various levels in the organization. Following discusses an overview of Training approach for e-Governance projects.

8.6.1 Overview of Approach for Training



1.Needs Analysis → 2. Gap Assessment → 3. Design Solutions → 4. Development → 5. Delivery → 6. Evaluation

Table below discusses each of the above activities in summary.

Activity	Description
Needs Analysis	Needs Analysis focuses on identifying the specific capabilities and skill sets required for various stakeholder groups in the context of e-Governance projects implementation. These skill sets including leadership, managerial, technical, domain, operational and other areas as relevant to the project. An understanding of the capabilities and skill sets is crucial to identify the gaps and to plan for bridging these gaps. The needs analysis will focus on defining the specific Knowledge, Skill and Attitude development requirements for the target stakeholder groups.
Gap Assessment	Gap assessment focuses on assessing the current capabilities and skill sets of the people across various levels vis-a-vis the target capabilities and skill sets needed in the context of e-Governance project implementation. Development of training plan and strategy will be performed based on these identified gaps.
Design Solutions	For the identified gaps, a training strategy/solution should be developed to address the Knowledge, Skill and Attitudinal requirements for the stakeholders. The solution should address the approach for development of KSA, methods of training, training course framework, detailed training plan, approach for evaluation of the training, development of training calendar etc.
Development	Development phase includes development of the relevant training material, training aids, feedback forms, student hand outs, faculty handouts and other training material as may be needed for conducting the training.
Delivery	Delivery phase includes imparting/conducting the training programs for various stakeholder groups as per the training calendar.

Evaluation	Evaluation phase includes evaluation of effectiveness of the training programs conducted to the stakeholders and improving the approach and training material based on the specific feedback back provided by the stakeholders.

8.6.2 Training Needs Assessment

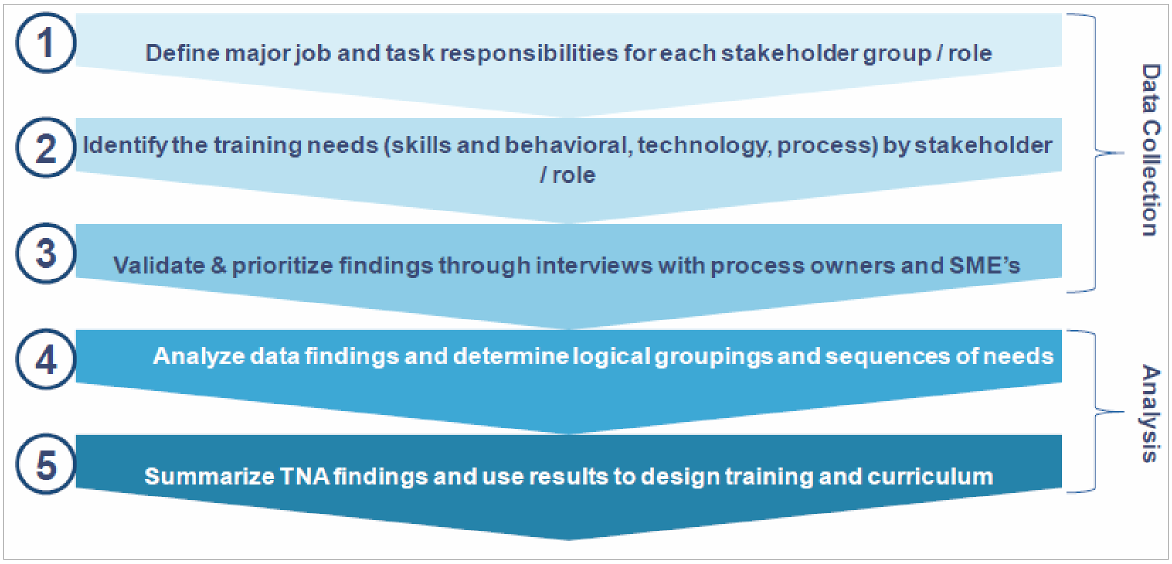
Training Needs Assessment/Analysis (TNA) focuses on identifying these skills/capabilities gaps in the employees of the organization, which will provide crucial input into development of a training plan/strategy. Following discusses some key objectives of the Training Needs Analysis (TNA):

- To understand the training audiences & their needs in the context of e-Governance
- To assess the training needs by role and by training type to address the knowledge and skills gaps :
  - Understand the changes to processes taking effect due to e-Governance adoption
  - Identify new technologies (or changes to existing technologies) taking effect
  - Assess new skills and behaviors needed to perform work in the new environment
- To identify areas requiring the greatest training focus and prioritizing training activities to address all critical dependencies
- To understand common training needs required for all stakeholders (internal / external)
- To outline potential skills and training risks to a successful go-live, and recommend mitigating actions

Following presents scope and overview of approach for conducting the Training Needs Assessment. Scope of TNA includes:

- Typically the scope of the TNA in an e-Governance project will include all process, technology, and Skills and Behavioral training, needed to ensure a successful implementation.
- TNA will cover all the stakeholders who will be impacted by the change
- The TNA will be a key input to designing the training strategy and interventions to ensure staff are sufficiently skilled to fulfill their roles in the changed environment.

Following summarizes the approach for TNA:



1 Define major job and task responsibilities for each stakeholder group / role

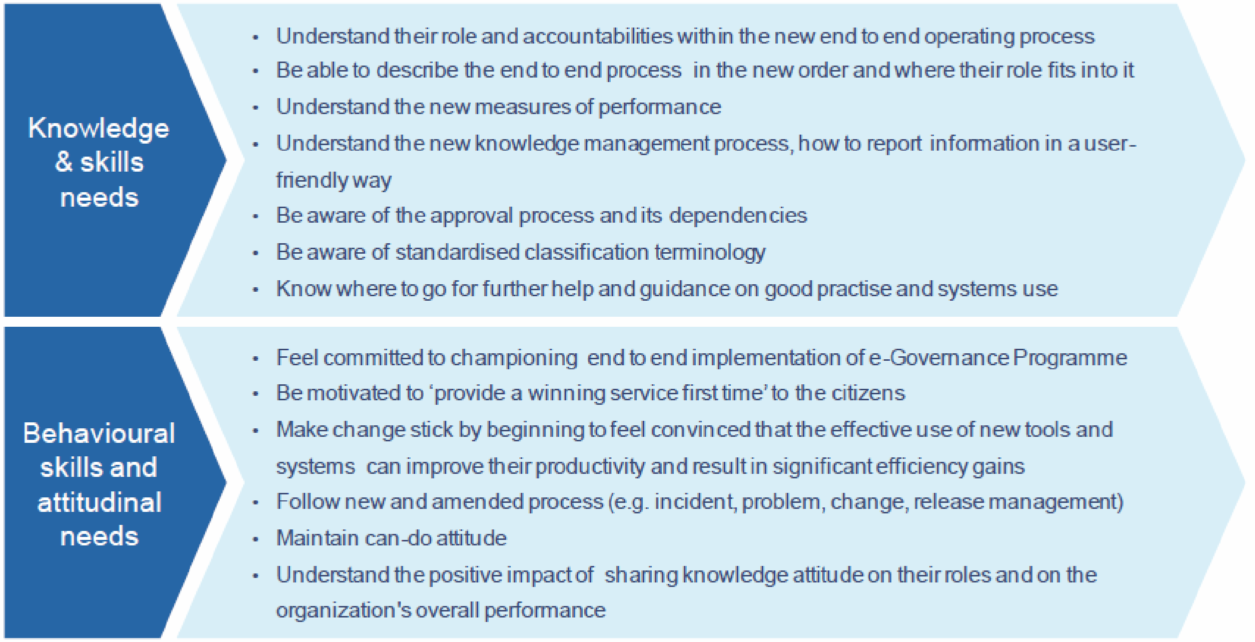
2 Identify the training needs (skills and behavioral, technology, process) by stakeholder / role

3 Validate & prioritize findings through interviews with process owners and SME's

4 Analyze data findings and determine logical groupings and sequences of needs

5 Summarize TNA findings and use results to design training and curriculum

A typical Training needs analysis output of the TNA includes:



Knowledge & skills needs

- Understand their role and accountabilities within the new end to end operating process
- Be able to describe the end to end process in the new order and where their role fits into it
- Understand the new measures of performance
- Understand the new knowledge management process, how to report information in a user-friendly way
- Be aware of the approval process and its dependencies
- Be aware of standardised classification terminology
- Know where to go for further help and guidance on good practise and systems use

Behavioural skills and attitudinal needs

- Feel committed to championing end to end implementation of e-Governance Programme
- Be motivated to 'provide a winning service first time' to the citizens
- Make change stick by beginning to feel convinced that the effective use of new tools and systems can improve their productivity and result in significant efficiency gains
- Follow new and amended process (e.g. incident, problem, change, release management)
- Maintain can-do attitude
- Understand the positive impact of sharing knowledge attitude on their roles and on the organization's overall performance

8.6.3 Assess Current Capabilities

Existing skill levels are assessed amongst the stakeholder groups and skill gap analysis is conducted based on future requirement from the role. This includes:

- Determine the effectiveness and ability of the organization’s present staff in completing the appropriate tasks to the required levels of competence.
- This information can be gained through a range of steps used in isolation or in combination depending on the size of the organization & the scale of change. e.g.
    - Self assessment
    - Line manager interview
    - Stakeholder interviews
    - Surveys or questionnaires
    - Existing MIS
    - On-job observation
    - Customer feedback

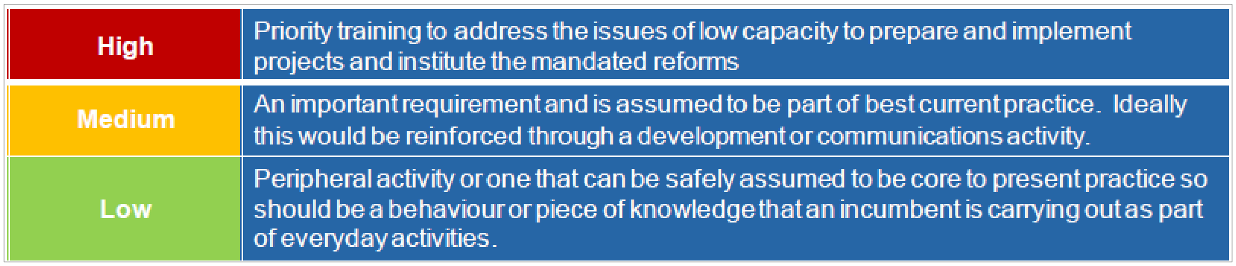
8.6.4 Compare Current and Target Competency Levels to Identify Gaps

- Identify and document gaps between current & required competency levels
- Record the gaps as potential training requirements
- Evaluate the potential training requirements to identify which are caused by a complete or partial lack of skills or knowledge and which have other causes. Then:
    - List as training requirements, those performance gaps caused by lack of skills/knowledge; and
    - List as issues those performance gaps not caused by lack of skills or knowledge
- Determine in a report possible non-training solutions e.g. changes in reward systems, amendments to service level agreements, geographic location of function and/or

stakeholder

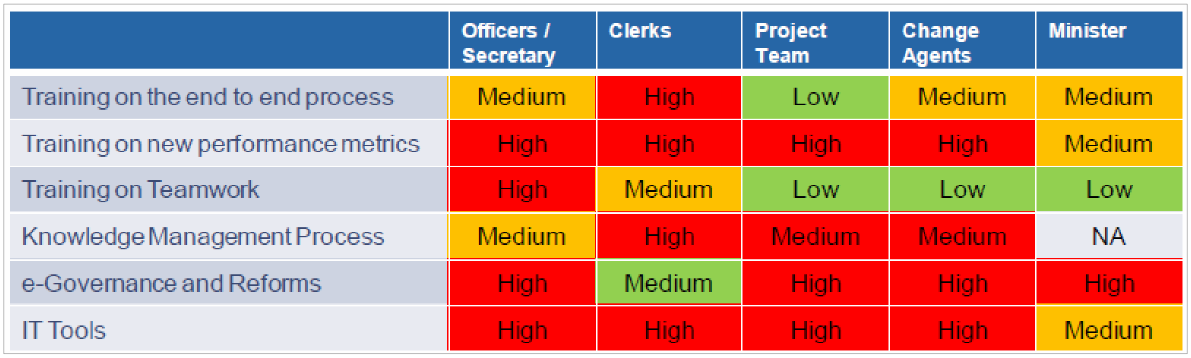
8.6.5 Identification of Skill Gaps

Identified skill gaps are then categorized as 'High', 'Medium' and 'Low' basis the importance and priority of the training.



High	Priority training to address the issues of low capacity to prepare and implement projects and institute the mandated reforms
Medium	An important requirement and is assumed to be part of best current practice. Ideally this would be reinforced through a development or communications activity.
Low	Peripheral activity or one that can be safely assumed to be core to present practice so should be a behaviour or piece of knowledge that an incumbent is carrying out as part of everyday activities.

Based on the identified training requirements, typically the training requirement for various stakeholder groups are prioritized as below. The table below is for Illustration only, the number of stakeholders and their categories would vary depending upon the scope and nature of the project.



	Officers / Secretary	Clerks	Project Team	Change Agents	Minister
Training on the end to end process	Medium	High	Low	Medium	Medium
Training on new performance metrics	High	High	High	High	Medium
Training on Teamwork	High	Medium	Low	Low	Low
Knowledge Management Process	Medium	High	Medium	Medium	NA
e-Governance and Reforms	High	Medium	High	High	High
IT Tools	High	High	High	High	Medium

8.6.6 Development of Training Scope and Strategy

The objective of developing a training strategy to focus on the training activity for the transformation program and determine the types of training to be conducted for each target audience. Components of a training strategy framework

- Approach to training
- Design,
- Development,
- Delivery
- Evaluation

The scope defines:

- The type and number of courses to be developed or changed
- The purpose and the likely number of training sessions required
- Initial assumptions and risks
- Any legislative and regulatory requirements
- High level training plan

The strategy determines:

- The training environment requirements;
- Statement of training principles and the objectives; macro content;
- Cost-effective range of delivery methods, e.g. classroom, face to face, e-learning,
- Approach to training management & administration;

- Any pre-requisites for training; and
- Approach to quality assurance.

8.6.7 Developing Implementation Plan

Based on the training scope and strategy, a training plan should be developed including the specific activities to be conducted for development of course, conducting training, training calendar etc. Following presents an overview of training plan.

8.7 Communications Management

Stakeholder communication is a critical aspect in ensuring stakeholder buy-in and acceptance of proposed policy, process, system and organizational changes. Communications Management addresses the need to engage, communicate and management of apprehensions and aspirations of the people impacted by the proposed process, system and structural changes. Moving to a new business environment, with changes in the structures, business processes and induction of automated systems, may put stress on the employees of the organization and other stakeholders, even when the envisaged outcomes for them are positive. Any major changes or impact to the current working environment may have severe impact to the people and hence will also impact overall functioning of government. Considering this, it is critical to communicate and prepare the employees for the change. Communications Management Plan, should address the specific communication and engagement needs for each stakeholder group, communication methods, messages, responsibilities etc.

8.7.1 Assess Stakeholder Engagement & Communication Needs

Stakeholder impact assessment and readiness survey provides key insights into the communication needs of various stakeholder groups impacted by proposed e-Governance initiative. In addition, department need to study the current Communication Approach & Methods adopted in the organization for the ongoing initiatives and need to assess the changes in the current approach/methods and to identify additional communications needs and methods for successful engagement of stakeholders and to receive buy in for proposed project implementation.

Current state assessment allows to identify what works well and what doesn't - and what new or innovative approaches could be used in the future. This will be useful for gaining an understanding of:

- Who is responsible for internal/external communication? Where are they based?
- Existing communication organizational charts / relationship diagrams
- Method(s) by which communications are developed, reviewed, approved and distributed
- The communication channels used / available. How successful are they? How is this measured?
- The methods staff / stakeholders use to provide feedback, and how often
- Current perceptions about the effectiveness of communication and why

8.7.2 Develop Stakeholder Engagement & Communication Plan

The stakeholder mapping and readiness assessment, as discussed earlier, provides critical inputs into the key stakeholders impacted, their role and influence in the e-Governance project. Based on these inputs, department need to evaluate/define the following for development of a communications strategy:

- Objectives of communication and engagement of each stakeholder
- Who needs to be communicated with, priorities and level of involvement is needed from each individual or group
- The key messages and how will they be tailored for each group
- Appropriate vehicle for conveying that message

- Ways to maintain stakeholder interest in the project / initiative throughout its duration
- Ways to listen to the stakeholder response and measurement approach to evaluate response

From these inputs, department will need to map the stakeholders into 'Know, Think, Feel, Do' map, which identifies Stakeholder group, what they should know from the e-Governance project, what the stakeholder group think/feel about the communicated change, what the stakeholder is required to do to successfully adopt the change.

Once department identifies what different stakeholders need to Know, Think, Feel and Do, department need to put together a Communication Strategy Framework outlining it will help its employees to get there. The Framework includes things like Communication objectives, Key messages, Roles and responsibilities, Guiding principles, Timings, Channels and media, Risks and Success measures.

For continuously updating and revising the communications and engagement plan is critical for project implementation and it requires incorporating feedback mechanisms from pilot phase/communications to make the process effective and inline with requirements on ground. Department need to define the feedback mechanisms needed, including communication evaluation survey; running periodic focus groups, working with the local change agents within the Change Network etc, for updating/refining the communications management plan. We will develop supporting tools/guidance material for obtaining feedback from stakeholder groups in this regard.

8.7.3 Implementation of Engagement & Communication Plan

In this phase, department will need to launch the engagement and communications activities based on agreed upon stakeholder engagement and communications plan. The specific activities performed in this stage include:

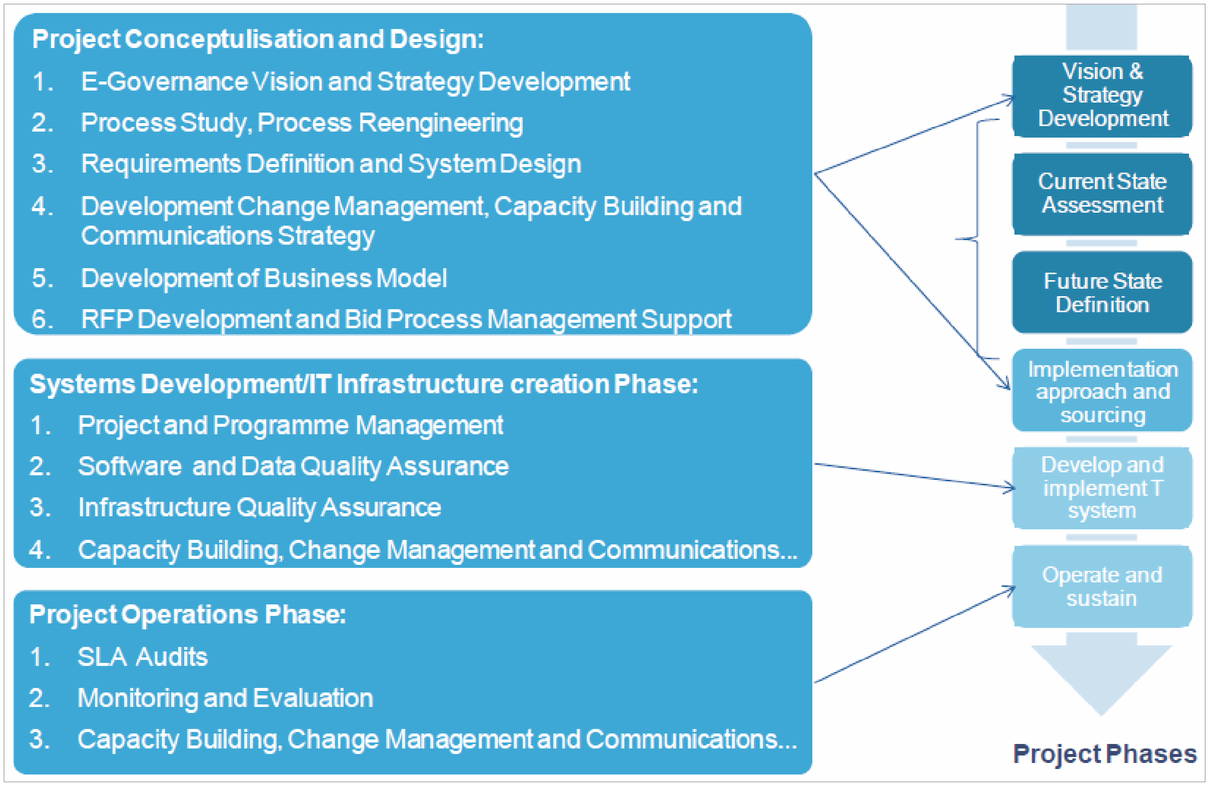
- Distributing materials via the appropriate channels, including populating a bespoke website and/or portal
- Managing communication activities, workshops, town halls and focus groups to deliver or facilitate face to face communication
- Implementing feedback and discussion channels and opportunities
- Coaching and supporting the Change Network and senior and local line management on their on-going communications and engagement role.

9. Business Models for implementation of e-Governance

e-Governance projects based on the objectives and scope would require various investments and for development of a business model it is imperative to have a clear understanding of the investments required in a project. Following discusses illustrative costs in various categories of e-Governance projects.

9.1 Costs in e-Governance Consultancy Projects

Following lists illustrative list of costs related to the consultancy services associated with various phases of e-Governance projects.



Project Conceptulisation and Design:

1. E-Governance Vision and Strategy Development
2. Process Study, Process Reengineering
3. Requirements Definition and System Design
4. Development Change Management, Capacity Building and Communications Strategy
5. Development of Business Model
6. RFP Development and Bid Process Management Support

Systems Development/IT Infrastructure creation Phase:

1. Project and Programme Management
2. Software and Data Quality Assurance
3. Infrastructure Quality Assurance
4. Capacity Building, Change Management and Communications...

Project Operations Phase:

1. SLA Audits
2. Monitoring and Evaluation
3. Capacity Building, Change Management and Communications...

Vision & Strategy Development

Current State Assessment

Future State Definition

Implementation approach and sourcing

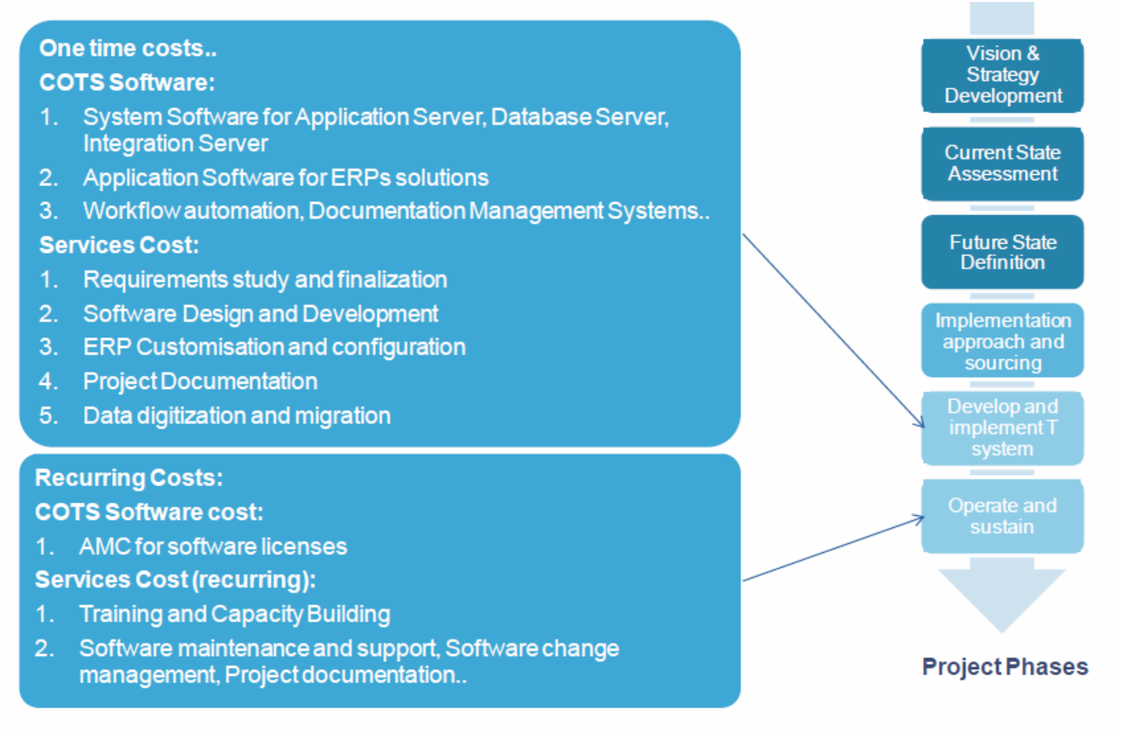
Develop and implement T system

Operate and sustain

Project Phases

9.1.1 Costs in e-Governance Projects - Software Design, Development and Maintenance

Following lists illustrative list of costs related to the software design, development and maintenance projects.



One time costs..

COTS Software:

1. System Software for Application Server, Database Server, Integration Server
2. Application Software for ERPs solutions
3. Workflow automation, Documentation Management Systems..

Services Cost:

1. Requirements study and finalization
2. Software Design and Development
3. ERP Customisation and configuration
4. Project Documentation
5. Data digitization and migration

Recurring Costs:

COTS Software cost:

1. AMC for software licenses

Services Cost (recurring):

1. Training and Capacity Building
2. Software maintenance and support, Software change management, Project documentation..

Vision & Strategy Development

Current State Assessment

Future State Definition

Implementation approach and sourcing

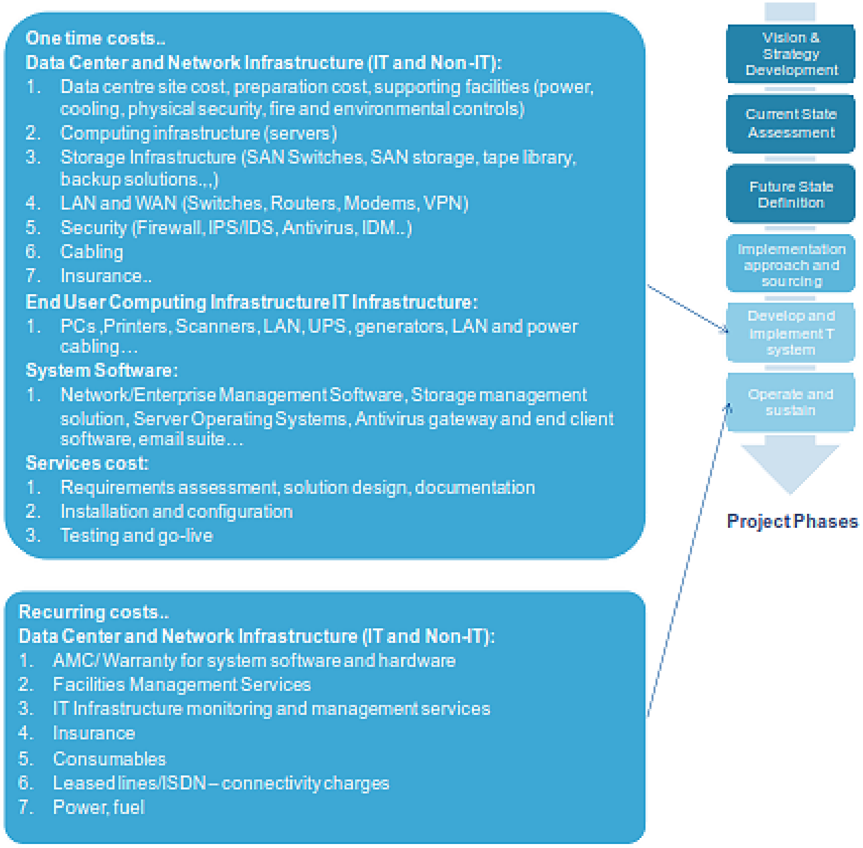
Develop and implement T system

Operate and sustain

Project Phases

9.1.2 Costs in e-Governance Projects - IT Infrastructure creation and maintenance

Following lists illustrative list of costs related to the IT Infrastructure creation and maintenance projects.



One time costs..

Data Center and Network Infrastructure (IT and Non-IT):

1. Data centre site cost, preparation cost, supporting facilities (power, cooling, physical security, fire and environmental controls)
2. Computing infrastructure (servers)
3. Storage Infrastructure (SAN Switches, SAN storage, tape library, backup solutions.,.)
4. LAN and WAN (Switches, Routers, Modems, VPN)
5. Security (Firewall, IPS/IDS, Antivirus, IDM..)
6. Cabling
7. Insurance..

End User Computing Infrastructure IT Infrastructure:

1. PCs ,Printers, Scanners, LAN, UPS, generators, LAN and power cabling…

System Software:

1. Network/Enterprise Management Software, Storage management solution, Server Operating Systems, Antivirus gateway and end client software, email suite…

Services cost:

1. Requirements assessment, solution design, documentation
2. Installation and configuration
3. Testing and go-live

Recurring costs..

Data Center and Network Infrastructure (IT and Non-IT):

1. AMC/ Warranty for system software and hardware
2. Facilities Management Services
3. IT Infrastructure monitoring and management services
4. Insurance
5. Consumables
6. Leased lines/ISDN – connectivity charges
7. Power, fuel

Vision & Strategy Development

Current State Assessment

Future State Definition

Implementation approach and sourcing

Develop and implement T system

Operate and sustain

Project Phases

9.2 Revenue opportunities in e-Governance projects

e-Governance initiatives also provide significant opportunity to the government departments in provision of value added services through new or enhanced service delivery channels to the customers. The scope of many e-Governance initiatives includes creation of digital data/information for critical areas such as properties, land records, tax payer records etc and this data provides significant opportunities for conceptualizing and delivering new services to the targeted stakeholders. However, usage and providing services using the digital data should be performed as per the applicable data protection and privacy acts and regulations in the country. These value added services and new service delivery channels provide revenue generation opportunities to the government departments, which can support in sustaining the project enhancements, operations and maintenance. Following provides illustrative examples of revenue generation opportunities provided by e-Governance initiatives. Sustain

- Portal registration/subscription charges
- Transaction fees for the online services
- Advertising revenue from the portal
- Advertising revenues from service center
- Fees for delivery of B2C and B2G services through common service centers
- Convenience fees - enhancement in the current fees/charges

Definition of service charges and transaction fees should also ensure that it is convenient to the service recipient.

9.3 Introduction to the Business Models

A Business Model is the description of the VALUE an Enterprise offers to its Customers, the financial model of the initiative and the network of Partners & their relationships for creating, marketing and delivering the value to generate profitable & sustainable revenue streams. The reasons for considering business model in e-Governance are as follows:

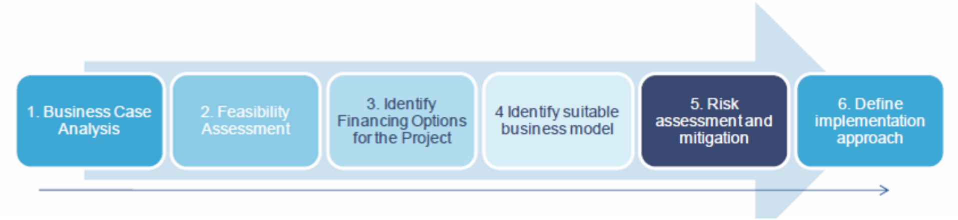
- To define the VALUE Proposition clearly
- To bring about clarity on roles & responsibilities of Government, Stakeholders & Implementing Agencies
- To ensure sustainability

A Business model, in summary, for a project should address/answer the following

- How much does it cost to create and maintain the project?
- Is the project feasible?
- Who is funding for the Project?
- Who is developing or implementing the project?
- Who is paying for the project?
- What are payment terms?
- Roles and responsibilities of the parties concerned with the business model
- Duration of the contract etc.

9.4 Approach for Development of Business Model

Following presents an overview of approach for development of business model for e-Gov projects.


1. Business Case Analysis
2. Feasibility Assessment
3. Identify Financing Options for the Project
4 Identify suitable business model
5. Risk assessment and mitigation
6. Define implementation approach

9.4.1 Step 1: Business Case Analysis

Business case analysis is aimed to:

- Assess the needs of the stakeholder
- Assess the need for the project
- Identify the project objectives and project benefits
- To define the outputs and outcomes of the project
- Assess the learning from similar implementations in the country and globally...
- Define the requirements and scope of the project
- In summary, to establish the business case for undertaking the project

Business case establishment for an e-Governance project can typically be performed during e-Governance vision and strategy development phase during which the specific need and objectives for an e-Governance initiative are defined.

9.4.2 Step 2: Feasibility Assessment

Feasibility Assessment is carried out in several ways:

- Justification for the project - is addressed through Business Case Analysis
- Technical feasibility of the project - addressed through solution evaluation and benchmarking with domestic and global experiences in similar context
- Financial feasibility
- Is the planned budget sufficient for the expected investments needed for the project (creation and maintenance) Or Can the project be undertaken within the available budgets?
- Are project budget, expected funding (including external funding sources) and revenues (services charges, transaction fees.) sufficient for project creation and maintenance?
- Is there sufficient market size for the private partner?
- Will this project be profitable for the private partners and will there be sufficient interest from private partners in the project?
- What should be viability gap funding to address the profit requirements of the private partners to achieve the minimum/standard Internal Rate of Return.?
- In most e-Governance projects financial feasibility assessment is not performed
- The project costs are estimated and necessary budgetary provisions are made based on the project cost or project features are modified to suit the budgeted project cost
- Financial feasibility assessment plays key role in
  - When a project is expected to provide returns to the government or the private implementation partner through user/service charges and
  - The investments and profits are expected to be realized through the services delivered through the created project etc.

In assessment of financial feasibility assessment, calculation of Net Present Value (NPV) and Internal Rate of Return (IRR) plays a crucial role. Following presents a brief overview of NPV and IRR.

Net Present Value

Generally, the duration of e-Governance projects are for longer periods i.e. approximately 3-5 years and requires continuous investments and cash flows required for the project. Net Present Value (NPV) represents the present value of the total project investments and cash flows required for the proposed e-Governance project over the entire project period. It works on the basic principle that a rupee today is worth more than a rupee tomorrow (a million rupees was a huge amount few years back, probably not of the same value currently). The Net present value depends upon the forecasted cash flows for the project and opportunity cost of the capital or expected rate of return.

NPV can be used to:

- To understand the Project Value in current terms with cash outflows spread across years
- To understand how much funding support may be needed for the project
- To assess the risk and rewards of the project
- To verify whether the project is lucrative enough to attract private sector efforts and investments
- To ensure that project concepts and designs don't fail in the field due to lack of financial feasibility.

Internal Rate of Return

Internal Rate of Return refers to the rate of return or discount rate at which Net Present Value equals to zero. IRR is used to calculate the expected rate of return for the investments required for creation and maintenance of the project. In general, project is acceptable if IRR is greater than the opportunity cost of capital.

IRR can be used to:

- To understand the expected rate of returns for the project
- To assess the potential for revenues and profits for the private sector partner
- To facilitate in identifying the viability gap funding or to allow the alternate revenue channels for private partner
- To ensure reasonable level of returns to private sector - not significantly high and not a loss making initiative.

Why Calculate NPV and IRR?

- To understand the Project Value in current terms with cash outflows spread across years
- To understand how much funding support may be needed from Government
- To assess the risk and rewards of the project
- To verify whether the project is lucrative enough to attract private sector efforts and investments
- To ensure that project concepts and designs don't fail in the field due to lack of financial feasibility

However, it is critical to understand that, in general, IRR focus for government and private sectors vary considering the role of both the parties.

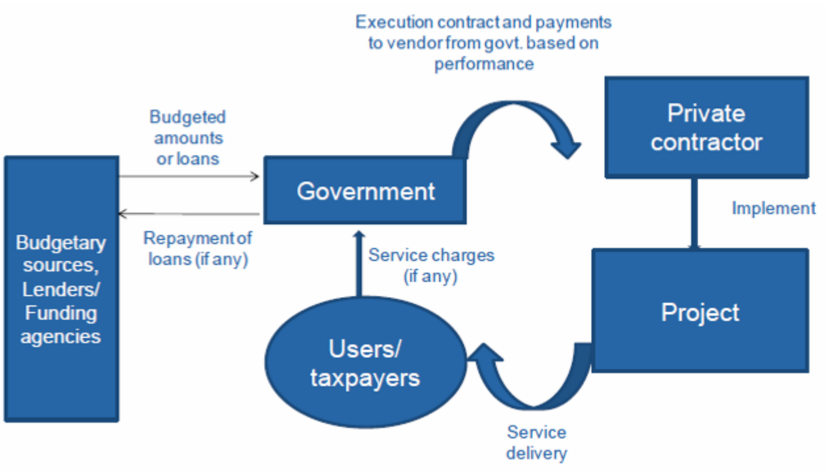
IRR focus for government, in general, focuses on:

- Achieving project objectives
- Economic development
- Social Welfare
- Better access to healthcare and education
- Improved service delivery
- Improved transparency
- Creation of quality infrastructure.

Whereas IRR focus for the private sector is focused on the financial gains and profits from the investments needed in project creation and maintenance. Based on the NPV and IRR, Government department can:

- Assess whether the project is financially feasible
- Assess the concessions, subsidies, gap funding, budgetary support or alternate funding resources needed for ensuring the private sector participation and project sustainability
- Identify the controls to ensure that unreasonably high returns are not accrued to the private partner - pass on the benefits to the government or end users (citizens.)

9.4.3 Step 3: Identifying Project Financing Option


Execution contract and payments to vendor from govt. based on performance
Private contractor
Budgeted amounts or loans
Government
Implement
Budgetary sources, Lenders/ Funding agencies
Repayment of loans (if any)
Service charges (if any)
Project
Users/ taxpayers
Service delivery

Before understanding various business models, it is critical to understand various project financing options for e-Governance projects. These are:

- Public Finance
- Private Finance
- Project Finance

Public Finance

In public finance model, government sponsors the project through budgetary sources or loans and the project is implemented through an execution contract with the private partner. This is a conventional process of project implementations by the government where payments are made to the private partner based on the quality of the services delivered in the project.

Execution contract refers to the contract with the private partner stating:

- Scope of services
- Commercials quoted during the bidding/vendor selection processes
- Payment terms
- Implementation/delivery schedule for the project
- SLAs
- And other terms and conditions of the project

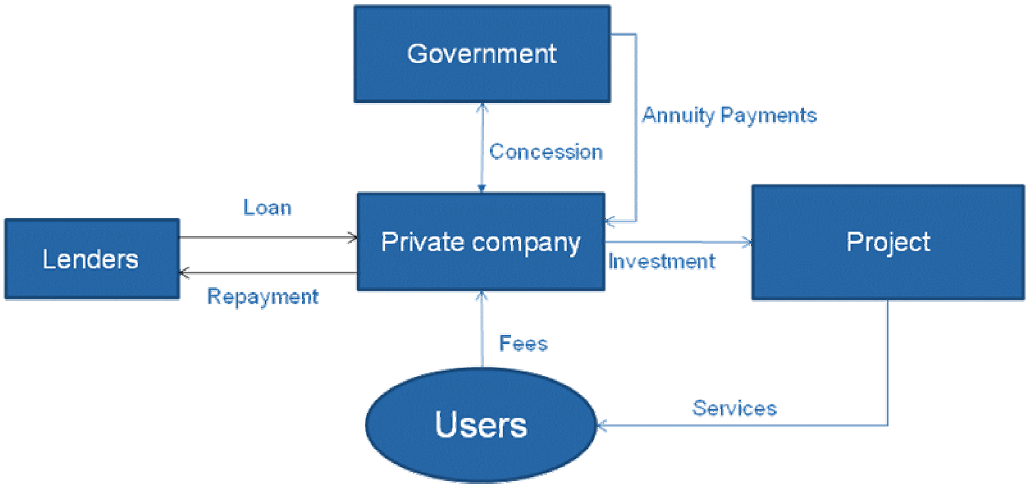
Where applicable, service charges are collected from the users by the government. However, it is critical to understand that the government is in the business of public service and not in all e-Government projects, the service charges can be collected by the government. Government can earn revenue from the service charges, where applicable. This diagram summarises the public finance option.

Private Finance

In this option, the project is financed by a private body through equity and debt and the revenue is generated for the private body through the user charges and/ or annuity payments by the government. Generally, this option is not suitable for capital Intensive projects as private organization do not like to strain its balance sheet through debt. Two important terms to understand in private finance are:

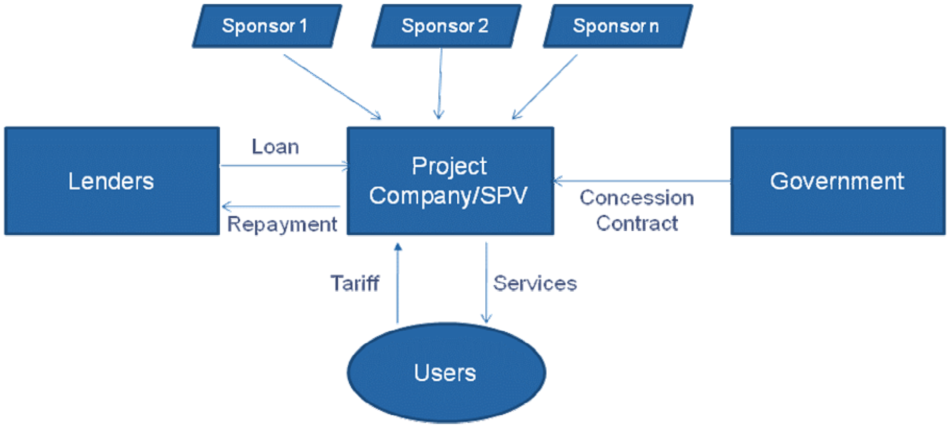
- Concession: The agreement between government and the private partner stipulating rights and responsibilities for the use of public assets.
- Concessionaire: The private partner with whom the government enters into concession agreement.

Following diagram summarizes private finance model.



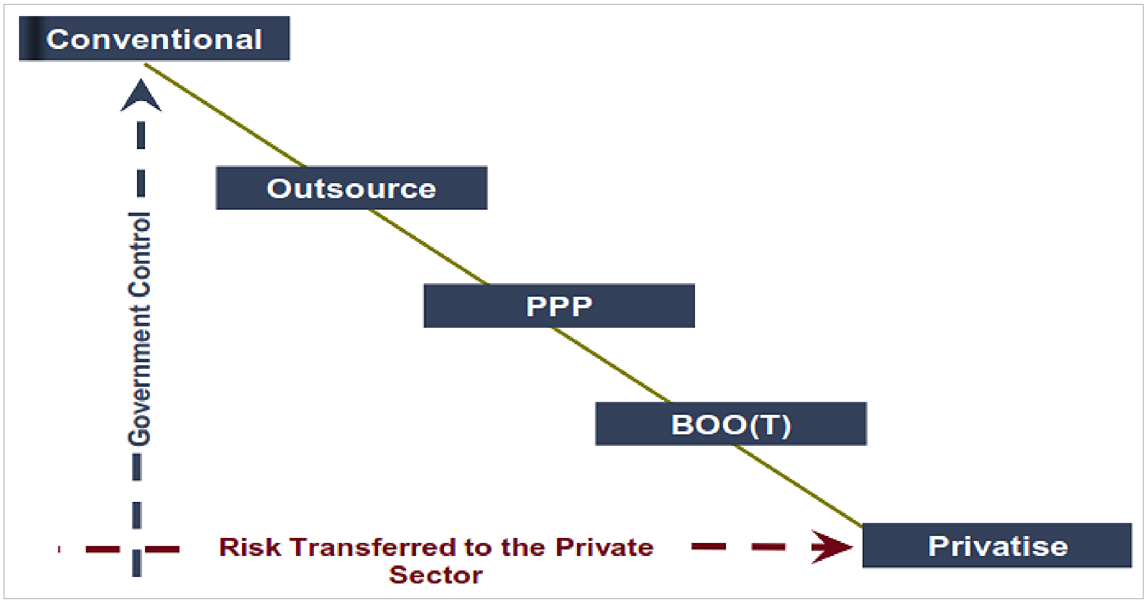
Project Finance

In project finance model, the project assets and its potential future earnings finance the project. In this model, generally a Special Purpose Vehicle is created which is legally independent and Debt financing is the primary source of funding for such projects. The risks are shared by participation of multiple complementing partners in the SPV and the concession agreement is signed with the SPV or the Project Company so formed for the project. Following diagram summarizes the project finance option.



9.4.4 Step 4: Evaluation of Business Models and Selection of Suitable Business Models

Following diagram presents various business models for implementation of e-Governance projects.



Business Model	Key Features
Conventional	• Government maintains complete control on the project creation, execution and assets • Government funds the project investments for the capital and operational expenditure during the project tenure • Government creates/develops the project • Government Maintains the project including operations and maintenance of the project • 100% of the project risk and returns are accrued to government only
Outsource	• Government maintains complete control on the project creation, execution and assets • Government funds the project investments for the capital and operational expenditure during the project tenure • Government leverages private sector strengths for creation of the project or maintenance of the project or both • Risks are allocated to the government and private sector based on the responsibilities (e.g. government will have the risk of project demand, the private sector will carry the risk of performance and quality of the services delivered to the government)

PPP	• The government does not need to own infrastructure to deliver services • The government retains political responsibility/accountability to deliver services for the community; • The government defines the timeframe in which the services must be delivered; and the quality and quantity of services needed; • The private sector delivers the services and finances or part finances the project; • Government provides the concessions for the private party, if needed • Private sector remunerated through services charges/transaction fees/gap funding. • Risks are allocated between the public and private sectors; • Various flavors of PPP exist with varying roles and responsibilities of public and private sectors
BOO(T)	• The government retains political responsibility/accountability to deliver services for the community; • The government defines the timeframe in which the services must be delivered; and the quality and quantity of services needed; • Private entity receives concession from government to finance, design, construct, implement and operate the project • Private sector is remunerated through services charges/transaction fees/gap funding. • The assets of the project are transferred to the government at the end of the concession period
Privatize	• The responsibility for delivery of services is completely transferred to the private sector • The ownership of the project or a business is completely transferred to the private sector • Government only regulates the functioning of the private sector

9.4.5 Step 5: Risk assessment and mitigation

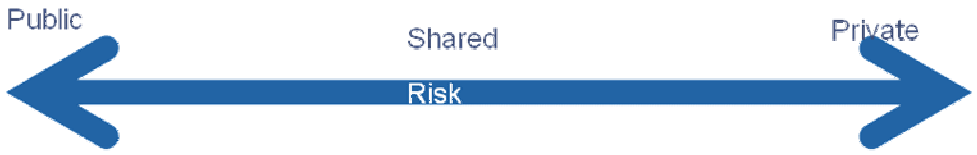
Risk assessment is a critical activity in a project implementation and selection of a suitable business model, which shall identify all the potential risks to the project. All the stakeholders must be aware of the potential project risks and a clear risk mitigation measures shall be identified, implemented and monitored throughout the project development and maintenance. The objective of risk assessment is to identify all the project risks and allocation of project risks to the suitable party who is well positioned and capable of managing the risks. Some typical project risks are surrounding:

- Land acquisition, planning and permissions
- Design
- Construction
- Commissioning
- Latent defects
- Operating performance
- Operating and maintenance costs
- Third party revenue
- Demand (volume)
- Residual value
- Inflation
- Regulatory
- Taxation

- Force Majeure
- Changes in requirement

Once risks are identified, the next step is to identifying the suitable entity to manage or address the risk. Minimizing the expected cost of risk is crucial for maximizing returns and risks should be allocated to the party best able to understand and manage them. Key considerations for risk allocation include:

- Who is best placed to reduce the probability of risk occurring?
- Who is best placed to manage the cost of risk if it does occur?



- Land acquisition, planning/permissions
- Demand risk (?)
- Changes in requirements
- Latent defects (existing)

- Inflation
- Regulatory
- Taxation
- Force majeure

- Design and construction
- Commissioning
- Operating and maintenance costs
- Operating performance
- Latent defects (new)
- Third party revenue

Table below presents an illustrative risk matrix.

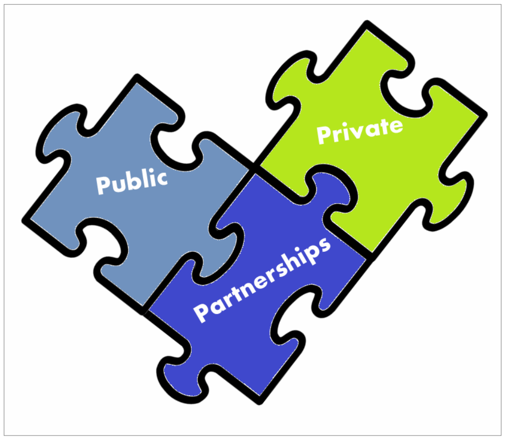
Risk	Description	Mitigation	Allocation
Availability of services	Possibility that Services provided by Private Partner do not meet output specifications of the Institution.	• Clear output specifications. • Performance monitoring. • Penalty Deductions • Payment linked to performance	Private Partner.
Risk of project completion	Delays, leading to cost overrun.	Develop implementation plan with tasks identified in detail, and monitor at sub task level.	Mostly to the private sector. Tasks like permissions and approvals to be allocated to the department
Design risks	Possibility that Private Partner's design may not achieve required output specifications.	• Clear output specifications. • Design warranty. • Patent and latent defect liability. • Third party review	Private Partner and the consultant for independent review

9.4.6 Step 6: Define Implementation Approach

Business model definition shall include a well defined implementation approach, which shall address the following key areas:

- Project management structure
  - Steering Committee structure
  - Project Management structure
- Identify the project phases
  - Project inception
  - Requirement definition
  - Design
  - Implementation
  - Stabilization
  - Support
- Identify project milestones in each of the phases
- Define the deliverables for each of the mile stones
- Payment structure
  - Payment linked to mile stones
- Budget provisioning
  - Financing model
  - Year wise allocation of funds
- Resource deployment
  - Capacity building
  - New recruitments
- Transition from private sector to department

10. Public Private Partnership (PPP)



e-Governance affects the lives of people of this world in many ways not only at the macro level but also at the micro levels. The flow of information of products, people, capital, and ideas offer great potential for radical improvements in human development, especially if these flows are enabled by ICT. Therefore, e-Governance has frequently demonstrated their potential for Public Private Partnership.

Public-private partnership (PPP) has emerged as a viable business model to counter these factors, apart from improving the economic sustainability of e-Governance projects. PPP describes a government service or private business venture which is funded and operated through a partnership of government and one or more private sector companies.

A public private partnership or PPP involves government and private sectors working together to deliver infrastructure or services that are traditionally provided by government. It involves private financing, construction and management of key infrastructure with the primary objective of improving public services.

While there is a need to create PPP deals, these need to be structured to ensure a win - win for all the stake holders. Sometimes it is also ambiguous whether the proposed PPP contract is, indeed in the PPP domain or not. PPP essentially implies sharing of risks and rewards of a venture. The basic features of PPP are:

- PPPs are concerned with services, not assets
- The government does not need to own infrastructure to deliver services
- PPPs are a procurement option, not a novel method of developing public infrastructure
- PPP policy sits alongside other procurement methods - i.e. conventional, outsourcing, leasing etc.
- Suitable to some public projects, not all projects
- Private partner investing in public infrastructure, and providing related non-core processes/services to the government or to the community on the government's behalf
- Government retaining responsibility for the delivery of core processes/services, and
- The government and private party working together under long-term arrangements, whereby the payments to the private sector party depend upon its continuing to deliver the specified services to the agreed performance standards. Failure to meet these standards results in the private partner not being paid

10.1 The Rationale for PPP

Governments decide on private sector participation with the following objectives:

- Possibility of cost-sharing projects, with a possible Return on investment for the private sector
- To bring technical and managerial expertise with technological developments in the new sector
- To improve economic efficiency in the sector in both operating performance and the use of capital investment
- To bring in large scale investment in the sector
- Private sector has invaluable expertise that can be tapped by government in the areas of

customer satisfaction, work productivity gains, and personnel efficiency.

- Possibility of technology transfer from the private to the public sector.
- While private sector participation will help in improving technical and managerial capacity, it will be effective only if the government chooses the appropriate form of PPP option and also supplements it with regulatory mechanisms.

10.2 PPP Benefits

10.2.1 PPP Benefits to Citizens

Some of the benefits which accrue as a result of the PPP model are:

- Easy access to services
- Single window/one-stop shop
- 24x7 convenience
- Flexibility in the choice of access methods and devices
- Saving of indirect cost and hardship
- Unity of responsibility leading to improved delivery of public services

10.2.2 Benefits to Government

- Allowing the government to concentrate on what it is good at
- Minimizing financial outgo
- Better liquidity
- Protection against technology obsolescence
- Speedier implementation of e-Governance projects
- Efficiencies in management and better exploitation of government assets, data
- Reduced Lifecycle costs of a project;
- Quantifying more accurately the costs of service delivery;
- Reduced risk of cost overruns;
- Increased revenues;
- Defining the scope and standards of service required, with timescales for development
- Maintaining a small government and a lean civil service;
- Spreading the government's capital works expenditure over the life of a project;

10.2.3 Benefits to Private Sector Partner

- Reliable streams of revenue
- Low risk
- Creation of employment in the development, implementation and delivery
- Capturing business from related sectors (wider market initiatives)
- Invoking private sector skills, experience, access to technology, and innovation

10.3 Key design principles for PPP

The following are the key principles that are important in defining government's relationship with the private sector in ways that are mutually beneficial.

- Respect "Return on Investment" (or ROI).For companies, this primarily means revenues. For government, this means efficient, reliable, robust services (and perhaps a share of revenues), and increased legitimacy and trust from citizens. For officials, this means receiving training, as well as professional opportunities and rewards for successful adoption of new procedures, work practices and responsibilities. ROI for officials is important as this will minimize "brain drain" from officials leaving government to join the private sector.

- Minimizing "brain drain" requires planning. To minimize government staff turnover, it is important to develop innovative compensation packages and professional perks as incentives. Government might also want to consider including clauses in contracts with the private sector that prevent contractors from hiring project staff away from government. Similarly, government employment contracts might prevent staff from leaving their jobs over a given period after receiving training or extra education.
- Create realistic business models for e-Governance projects. Companies need to sell e-Governance projects to their management, just as government needs to "sell" these projects to the public and to government officials. The partnership can be stronger if there are people in government who understand how companies work and people in the private sector who understand the needs of government. A solid, well-designed business plan will help.
- Find each partner's strengths. Both business and government need to contribute actively to the partnership. Companies can be a source of cost-sharing, technology and project management expertise. Government needs to promote the use of e-Governance among the public and officials, as well as create a legal framework. It must create incentives to help local companies grow and become viable partners in e-Governance.
- Develop formal policies on outsourcing. Government must establish clear parameters for working with the private sector. Outsourcing requires government to use and develop new types of contracts-with clear benchmarks of performance- that will not only ensure the delivery of goods and services, but also measure the performance of vendors and the quality of services received. More important, the bureaucracy needs to be trained on how to negotiate and draft such contracts.

10.4 Role of Various Partners

A PPP project involves collaboration between various types of private sector companies and the public agency. The PPP deal should be structured to be mutually beneficial to all the parties involved, with each party taking on the responsibilities which it is best able to manage. The roles of the Government and a private sector partner are described for a typical PPP project.

10.4.1 Role of Government in PPP

- Set policy, identify opportunities, and define objectives;
- Decide amongst competing priorities for public resources;
- Ensure transparency and probity in the procurement process;
- Identify needs in terms of output specifications that encourage flexibility and innovation in the manner of performance;
- Set and ensure the achievement of standards;
- Establish, monitor and enforce the levels of service;
- Ensure value for money is achieved;
- Determine and manage reward mechanisms and tariff structures;
- Identify and propose the allocation of risks;
- Provide a clear regulatory framework and perform regulatory functions; and
- Safeguard the interests of customers and the general public.

10.4.2 Role of Private Partner

- Achieve defined levels of performance in service delivery;
- Provide expertise and innovation;
- Provide access to private financing, as appropriate; and
- Provide a sufficient return to investors and other stakeholders.

10.5 Options for PPP

Arrangements with the private sector could be either through very simple transactions or through sophisticated and complex transactions. These options can be classified based on the nature of responsibility held by the government and the private sector. In some cases, the government maintains full responsibility of operations, maintenance and service, while in other cases; the government creates a framework wherein the private sector takes the full responsibility including investments. Such a framework is essentially created to protect consumers from monopolistic pricing and enforce standards. The various options are distinguished by the allocation of responsibility in terms of asset ownership and capital investment between the private and public sector.

10.5.1 Management Contracts

The government transfers the responsibility of operation and maintenance of its businesses to the private sector through a Management contract. The private sector will not be involved in any capital expenditure. Such contracts are given out for a period of 3-5 years. These are most effective where the main objective of the government is to rapidly enhance its technical capacity and its efficiency in performing specific tasks, or to prepare for greater private involvement. These contracts do not transfer commercial risks of the function assigned to the private operator and is a first good step for the government towards a full-fledged private sector involvement. Legally, there is no partnership between the government and private sector in a Management contract model.

Management contracts could be either very simple or complex. The performance of the private operator is monitored by the government and in many cases, fees is also linked to the success of the operation.

More often than not, the success of the operation depends not only on the private operator's ability to operate and maintain, but also on the government's ability to make the resources available. There is often a fine dividing line between operations and maintenance expenditures, for which the private operator is responsible and capital investment, for which the government is responsible-and both will affect the operator's performance. This option is however not a good one if a government wants to access private finance for new investments.

10.5.2 ASP Model - Application Service Provider model

The ASP 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-Governance initiatives that involve

- A requirement to launch the services in a short time frame.
- The technology is not complex and widely accepted and practiced in the private sector
- The nature of information is not so critical to governance.

Most often the ASP model is useful to leverage the existing ICT infrastructure and management skills already established by service providers. This creates a win-win situation by enabling the optimum utilization of ICT by leveraging the infrastructure already set up in the private sector and thereby reducing the transaction cost to the government/citizen.

10.5.3 BOOT -Build-Own-Operate-and-Transfer-model

BOOT is an arrangement between the government and the private sector where the private firm undertakes to build, operate, maintain and later on transfer the asset to the government. 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.

During the period of the contract, say for 20-30 years, the government will pay a fee to the private operator. The contract between the BOOT concessionaire and the government is usually on a take-or-pay basis, thus placing demand risks on the government. Alternatively, the government and the private sector may arrange to share the risk where the government pays an additional charge.

10.5.4 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 - also known as the concession period. The revenue model of the project is either based on transaction charges (paid by the citizen or the government) or on EQI/EMI (Equated Quarterly Instalment/Equated Monthly Instalment) 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 physical infrastructure like service Centre(s) for delivering services to the citizens. Good examples are e-Governance projects relating to issue of driving licenses, registration of vehicles, and provision of integrated services to citizens across the counter.

10.5.5 JV Model

In this model, an SPV (Special Purpose Vehicle) is formed to undertake the e-Governance 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.

10.5.6 How to structure and Implement PPP

The following table provides an overview of the process to implement a typical PPP project.

Phase	Steps	Outcome
Step One : Vision	• Identify appropriate projects • Prioritize projects • Include in the budget process	• Clear vision of the concept
Step Two : Project Definition	• Define selected project • Identify investment requirement • Document transactions and volume • Define output based requirements • Undertake an Options analysis • Select type of PPP	• Project definition and preferred PPP structure
Step Three : Define project roles and responsibility	• Appoint project management team • Development project management plan • Identify critical decisions	• Dedicated project management structure in place, including transaction advisor

Phase	Steps	Outcome
Step Four: Feasibility study	- Document the costs, benefits and risks inherent in the government-funded option. - Address legal/legislative hurdles. - Consider the opportunities for risk transfer. - Identify range of options. - Approach the market to determine the nature of the private sector's interest. - Elaborate on the identified options by incorporating the information gained from the market. - Evaluate qualitative impacts, costs, benefits and risks. - Conduct quantitative whole-of-life financial evaluation. - Develop a Public Sector Comparator (PSC). - Ensure that the PSC incorporates all the efficiencies in service delivery that could realistically be achieved for that option. - Compare PPP option with the PSC on a value for money basis. - Demonstrate - Affordability - Risk transfer - Value for money - Identify preferred option	- Analytical framework supporting the preferred PPP option.
Step Five: RFQ	- Prepare Request for Qualifications - (RFQ) document. - Disseminate to wide audience. - Narrow respondents to short list.	- RFQ, which is written to elicit a strong response from the private market.
Step Six: RFP & draft contract	- Prepare Request for Proposals (RFP) - Disseminate with draft contract short list. - Allow scope for innovation in service delivery.	- RFP, which is written to allow for innovative ideas, from the private sector.
Step Seven: Select preferred bidder	- Evaluating proposals for value for money, - Compare to PSC and to each other. - Perform adequate due diligence. - Select bidder based upon evaluation.	- Private sector partner to share risk and reward.
Step Eight: Formalize contract	- Negotiate contract with the selected private sector partner - Clarify desired outcomes and payment mechanism. - Execute contract.	- Performance-based and output driven contract.

Phase	Steps	Outcome
Step Nine: Commence project	• Transfer responsibility of operation. • Allow for implementation of systems, processes and payment mechanism. • Establish project monitoring and control.	• Smooth roll out, as per contractual specifications

11. Legal and policy framework for e-Governance implementations

11.1 Legal Aspects of e-Commerce and e-Governance

Ministry of Information Technology, Government of India, defines e-Governance as ". the application of Information Technology to processes of government functioning to bring about a Simple, Moral, Accountable, Responsive and Transparent governance". In other words, e- Governance uses Technology tools in government functioning and service delivery.

Use of Technology in government gives rise to many legal questions, like the validity of electronic transactions, electronic records and contracts, data protection and privacy etc. These legal aspects are in turn also relevant to the wider e-Commerce landscape of the country. These aspects should be addressed in the country's legal framework, in order to provide the sufficient legal backing to e-Commerce and e-Governance.

The Legal Framework also includes legislations in the domain, which may need amendments as part of e-Government roll-out.

11.2 Legal & Regulatory Framework in India

The components of Legal and Regulatory Framework in India for addressing these requirements is listed below. Each of these components is discussed in further details in subsequent chapters:

- Legislation in Information Technology domain:
    - IT Act, 2000
    - IT Act Amendments 2008
    - Rules under IT Act
- Implication of existing Laws vis-a-vis IT practices:
    - Indian Penal Code, Indian Evidence Act, IPR related laws (Copyright, Trademark, Patent etc)
- Legislation in the domain in which the e-Governance project is undertaken
- Guidelines for e-Governance under National e-Governance Plan (NeGP)
- Specific issues like legal implications of Portal based service delivery

The major legislation in the e-Commerce domain in India is the IT Act, 2000, which overrides previous legislations, in providing recognition to electronic records, transactions etc at par with their manual counterparts. The details of the Act are covered in the next section.

11.3 Information Technology Act, 2000

11.3.1 Background on IT Act, 2000

The Information Technology Act came into effect from October 17th, 2000. The Act was framed on the lines of the UNCITRAL Model Law, and India was the 12th nation in the world to adopt Cyber Laws.

The Act contains 94 Sections segregated into 13 Chapters and 4 Schedules. IT Act 2000 was amended through the Information Technology Amendment Act, 2008 which came into effect from October 27, 2009

11.3.2 Objectives of IT Act, 2000

The objectives of the IT Act are summarized below:

- Legal Recognition for transactions carried out by means of electronic data interchange
  - Digital Signatures and Regulatory Regime for Digital Signatures
  - Admissibility of Electronic Documents at par with paper documents
- e-Governance
  - Electronic Filing of Documents and e-Payments
- Define Civil wrongs, Offences, punishments
  - Investigation, Adjudication of Cyber crimes
  - Appellate Regime
- Amend existing Acts to address IT Act provisions
  - Indian Penal Code & Indian Evidence Act - 1872
  - Banker's Books Evidence Act - 1891 & Reserve Bank of India Act - 1934

11.3.3 Applicability to the Act

Exceptions of applicability to the Act, is extended to the following:

- A negotiable instrument (other than a cheque) as defined in section 13 of the Negotiable Instruments Act, 1881
- A power-of-attorney as defined in section 1A of the Powers-of-Attorney Act, 1882
- A trust as defined in section 3 of the Indian Trusts Act, 1882
- A will as defined in clause (h) of section 2 of the Indian Succession Act, 1925 including any other testamentary disposition
- Any contract for the sale or conveyance of immovable property or any interest in such property
- Any such class of documents or transactions as may be notified by the Central Government

The Act applies to the whole of India and also applies to any offence or contravention there under committed outside India by any person irrespective of his nationality, if such act involves a computer, computer system or network located in India.

The Act has superseding effect over existing legal provisions. Section 81 of the Act states that this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force. Only exceptions provided to the overriding effect are for the Copyright Act, 1957 or Patents Act, 1970.

11.3.4 Major Components of IT Act

The major areas addressed by the IT Act are listed below:

- Admissibility of electronic records at par with handwritten records
- Attribution, Acknowledgement and Receipt of Electronic Documents
- Authentication of electronic records
- Digital Signatures and Digital Signature Regime
- Cyber crimes and contraventions
- Amendments to other Acts (Indian Penal Code, Indian Evidence Act) These areas will be

discussed individually in the subsequent sections.

11.3.5 Recognition of electronic records

One of the main requirements of all e-Government and e-Commerce activities is the recognition of electronic / digital records at par with handwritten records. This recognition is extended by provisions of Chapter III of IT Act, 2000.

As per the definition provided in IT Act, 2000

> "Electronic record" means date, record or date generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche"

Section 4 of the IT Act provides legal recognition to electronic records

> "If any information is required in printed or written form under any law the Information provided in electronic form, which is accessible so as to be usable for subsequent use, shall be deemed to satisfy the requirement of presenting the document in writing or printed form"

The Act also provides for the use of electronic records in government service delivery. Section 4 of the Act specifies that in cases where:

- The filing of any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in a particular manner;
- The issue or grant of any license, permit, sanction or approval by whatever name called in a particular manner;
- The receipt or payment of money in a particular manner; Such requirement shall be deemed to have been satisfied:

  If such filing, issue, grant, receipt or payment, as the case may be, is effected by means of such electronic form as may be prescribed by the appropriate Government

These clauses allow for e-filing of documents, issue of certificates / licenses online and e-Payments, in government scenario. The Law also gives recognition for publication of Rules, Regulation etc in Electronic Gazette.

In cases where the signature of the individual is required (e.g. signing of application form), such requirement can be fulfilled by using Digital Signatures. Digital Signature regime is discussed in detail in a subsequent section.

The Act also provides for the conditions to be met in regard to retention of electronic records. According to Section 7 of the Act, any law provides that documents, records or information shall be retained for any specific period, then, that requirement shall be deemed to have been satisfied if such documents, records or information are retained in the electronic form, if:

- The information contained therein remains accessible so as to be usable for a subsequent reference;
- The electronic record is retained in the format in which it was originally generated, sent or received or in a format which can be demonstrated to represent accurately
- The details which will facilitate the identification of the origin, destination, date and time of dispatch or receipt of such electronic record are available in the electronic record

11.3.6 Attribution, Acknowledgement and Receipt of Electronic Documents

In dealing with electronic records, it is essential to have clear guidelines regarding attribution to an originator of the record. An electronic record can be attributed to the originator:

- If it was sent by the originator himself
- By a person who had the authority to act on behalf of the originator in respect of that electronic record; or
- By an information system programmed by or on behalf of the originator to operate

automatically.

Thus, an e-mail sent an individual can be attributed to him / her. Another important concept is the acknowledgement of receipt by the receiving party. An electronic record can be considered as received by the addressee:

- If Originator has not specified particular method - Any communication automated or otherwise from the addressee or conduct from the addressee indicating the receipt of the record
- If specified that the receipt is necessary, then unless acknowledgement has been received Electronic Record shall be deemed to have been never sent
- Where acknowledgement is not received within time specified or within reasonable time the originator may give notice to treat the Electronic record as though never sent

Another legal aspect in electronic transaction is the date, time and place of dispatch and receipt of electronic records. Following are the provisions in IT Act, specifying the date and time of dispatch and receipt.

- Unless otherwise agreed dispatch occurs when Electronic Record enters computer resource outside the control of originator
- If addressee has a designated computer resource, receipt occurs at time Electronic Record enters the designated computer. If electronic record is sent to a computer resource of addressee that is not designated, receipt occurs when Electronic Record is retrieved by addressee
- If no Computer Resource designated - when Electronic Record enters Computer Resource of Addressee
- Shall be deemed to be dispatched and received where originator has their principal place of business otherwise at his usual place of residence

11.3.7 IT Act Amendments, 2008

The IT Act, 2000 was amended in 2008 to include additional provisions, and also to correct certain provisions. The major changes introduced in the IT Act Amendments, 2008 were to:

- To make the Act Technology Neutral:
  - Enabling provision added to replace Technology specific "Digital Signatures" to technology neutral "Electronic Signatures". Central government to specify accepted forms of electronic signatures in the Rules
- To enable the IT Act to be easily amendable with advances of Technology
  - Exclusion of applicability modified to allow Central Government to change the list by executive orders (Rules)
- Enabling provision for PPP in e-Governance service delivery
- Provisions for more extensive coverage of Cyber Crimes including Cyber Terrorism

The changes in the Digital Signature Regime to introduce Electronic Signatures, is discussed in the next chapter.

A number of provisions were added in the amendments, to facilitate Public Private Partnership in government service delivery. These provisions include:

- **Section 6A(1):** The government may, for efficient delivery of services to the public through electronic means authorize, by order, any service provider to set up, maintain and upgrade the computerized facilities and perform such other services as it may specify, by notification in the Official Gazette
- **Section 6A(2):** The government may authorize any service provider authorized under

6A(1), to collect service charges as prescribed by government, from the person availing the service

- **Section 6A(3):** Subject to 6A(2), service charges may be collected, notwithstanding the fact that there is no express provision under the Act, rule, regulation or notification under which the service is provided to collect, retain and appropriate e-service charges by the service providers.
- **Section 6A(4):** Government shall specify the scale of service charges to be collected, by notification in the Official Gazette

These provisions are put in place to allow for innovative Business Models for PPP based service delivery.

11.3.8 Electronic Contracts

The IT Act Amendments provide legal recognition to contracts formed electronically. Section 10A of the IT Act states that:

> "Where in a contract formation, the communication of proposals, the acceptance of proposals, the revocation of proposals and acceptances, as the case may be, are expressed in electronic form or by means of an electronic record, such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose"

This provision, read along with the terms of the Indian Contract Act, 1872 provides recognition to contracts arrived at by electronic means. As per the Contract Act, the pre-requisites for a Contract are the following:

- An offer needs to be made
- The offer needs to be accepted
- They has to be lawful consideration
- There has to be intention to create legal relations
- The parties must be competent to contract
- There must be free and genuine consent
- The object of the contract must be lawful
- There must be certainty and possibility of performance

Section 10A allows for all these provisions to be fulfilled electronically.

11.4 Digital Signature Regime

11.4.1 Introduction to Digital Signatures

Digital / Electronic Signatures are the electronic equivalents of the handwritten signatures. Handwritten signatures fulfil the criteria that a manually signed document can be attributed to the individual, as the signature is unique to the person (authenticity, non repudiation and integrity). There are many electronic signature technologies, which allow signing electronic records, fulfilling the required criteria.

Recognition to Digital Signatures is provided by Section 3 of the IT Act. According to the section:

- Any subscriber may authenticate an electronic record by affixing his Digital Signature
- The authentication to be affected by use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record
- The private key and the public key are unique to the subscriber and constitute functioning key pair
- Verification of electronic record possible using public key of the subscriber

Section 5 of the Act establishes equivalence of Digital and Handwritten signature.

The exact type of Digital Signature to be used is not specified in the IT Act. Section 10 of the Act confers the authority to Central Government to prescribe Digital Signature Regime using Rules drafted under IT Act, 2000. These powers include the powers to prescribe:

- The type of digital signature;
- The manner and format in which the digital signature shall be affixed;
- The manner or procedure which facilitates identification of the person affixing the digital signature;
- Control processes and procedures to ensure adequate integrity, security and confidentiality of electronic records or payments;
- Any other matter which is necessary to give legal effect to digital signatures.

Accordingly, the following provisions were brought about by the Central Government in the IT (Certifying Authorities) Rules, 2000:

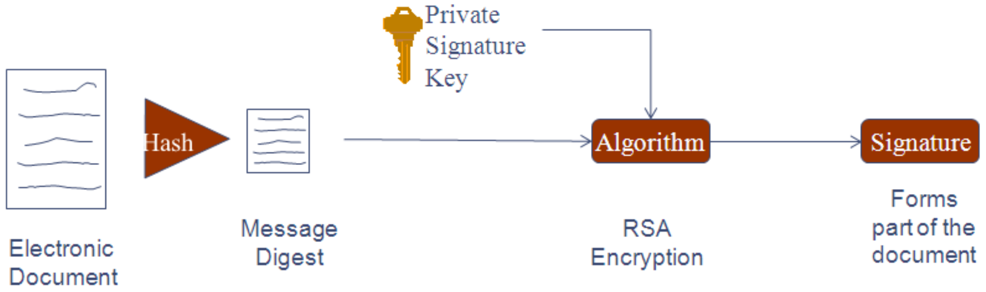
- "Digital Signature shall be created and verified by cryptography that concerns itself with transforming electronic record into seemingly unintelligible forms and back again";
- Public Key Cryptography to be used for creation and verification of Digital Signatures
- Prescribes ITU X.50g version 3 standard of Digital Signatures
- Defines the Digital Signatures Regime including guidelines for Licensed Certifying Authorities

Thus, Public Key Infrastructure (PKI) was the recommended standard for Digital Signatures in India as per the IT Act, 2000. The Act also describes the Institutional structures for governing the Digital Signature Regime.

11.4.2 PKI Based Digital Signature Basics

Public Key Cryptography is a form of cryptography in which each user has a private key and an associated public key. Distinct public / private key pairs may be used for either signing a message or for data encryption. Senders sign with their private key and encrypt with the recipient's public key. The public and private keys are 2048 bit keys (including algorithm identifier).

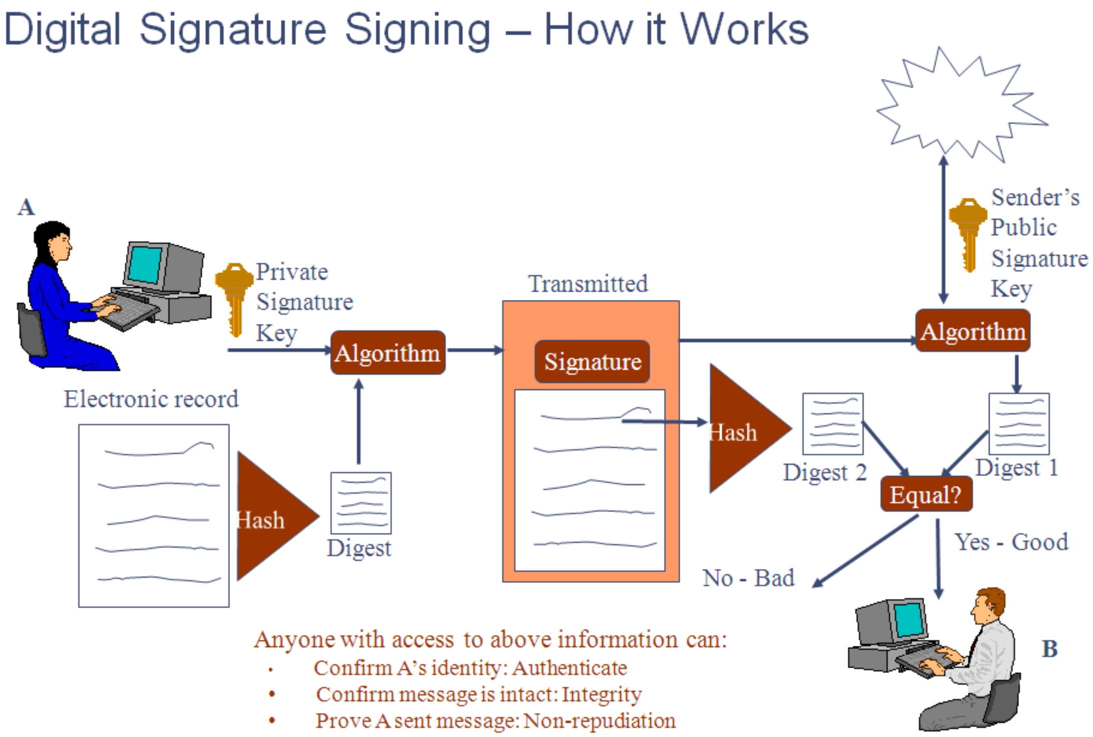
The figure below explains what a PKI based Digital Signature is:



Any message irrespective of its length can be compressed or abridged uniquely into a smaller length message called the Digest or the Hash. Smallest change in the message will change the Hash value of the message digest. The hash value is encrypted with the private key of a person is his digital signature on that e-Document. The following aspects may be noted:

- Digital Signature of a person therefore varies from document to document thus ensuring authenticity of each word of that document.
- As the public key of the signer is known, anybody can verify the message and the digital signature

Figure below shows how the digital signature is verified:



Anyone with access to above information can:

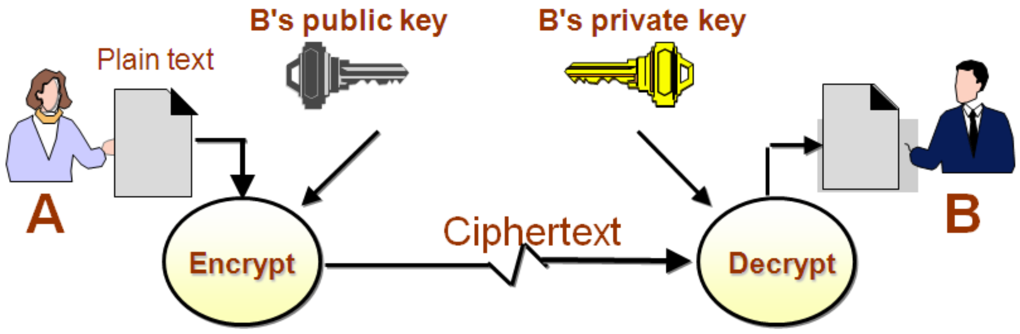
- Confirm A's identity: Authenticate
- Confirm message is intact: Integrity
- Prove A sent message: Non-repudiation

The electronic record with the sender's Digital Signature is received by the addressee. The addressee can then check the message digest with the digest obtained by using the sender's public key. If these two digests match, the addressee can be assured that the document has been sent by the sender. In case any changes have been made to the document in transit, the digests won't match ensuring integrity of the document.

The security services fulfilled by the Digital Signature are the following:

Service	What it means	How it is fulfilled
Privacy / Confidentiality	Protection against access by unintended recipients	By encryption using the recipient's Public Key
Authenticity	Proof that the sender is actually who he claims to be	By signing using the sender's Private Key, which can be verified by the recipient using the sender's public key
Non Repudiation	Proof that the sender has actually sent the signed message	
Integrity	Any changes in the original signed message should be detected	

Digital Signatures are also used for encrypting electronic records, as shown below:



In Digital Signature based encryption:

- A sends confidential data to B, knowing that only B can decrypt what is sent
- A encrypts with B's public key (openly available)
- B decrypts with his own private key (kept secret)

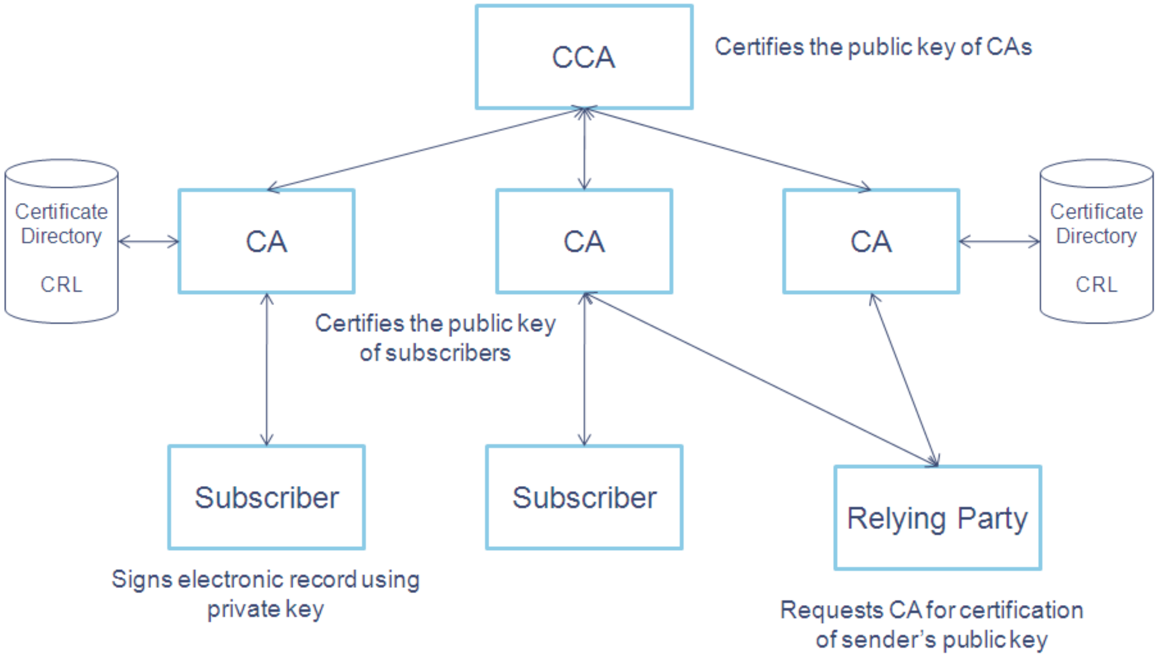
Such encryption finds application in many e-Governance contexts, including encryption of Commercial Bids in e-Procurement.

11.4.3 PKI Infrastructure

The PKI Infrastructure includes all mechanisms required to securely issue, distribute, and manage certificate based public keys, form the PKI Infrastructure. These include:

- Certifying Authority Architecture
- Secure Facilities
- Applications
- Policies and Procedures
- People

The PKI hierarchy in India is depicted below:


CCA
Certifies the public key of CAs
Certificate Directory
CRL
CA
CA
CA
Certificate Directory
CRL
Certifies the public key of subscribers
Subscriber
Subscriber
Relying Party
Signs electronic record using private key
Requests CA for certification of sender's public key

As indicated, the PKI hierarchy includes the following players:

Controller of Certifying Authorities (CCA)

- Set up as per IT Act, 2000 to license and regulate the working of Certifying Authorities
- Lay down standards and conditions governing Certifying Authorities and specify various forms and content of Digital Signature Certificates
- Certifies by the Public Key of the licensed CAs by operating the Root Certifying Authority of India (RCAI) key

Licensed Certifying Authorities

- Agencies authorized by CCA to issue Digital Signatures Certificates to end users and to certify the public key of the subscriber
- Must have well defined Identification process before issuing the certificate
- Provides online access to all the certificates issued
- Provides online access to the list of certificates revoked (Certificate Revocation List)
- Displays online the license issued by the Controller
- Must adhere to IT Act/Rules/Regulations and Guidelines

Registration Authorities

- Agencies authorized by CA for operational activities like face to face verification, registration of certificate information etc
- The RA is subsumed in the CA, and total responsibility for all actions of the RA is vested on the CA

Subscribers

- End users who apply for Digital Signature Certificates to Licensed CAs

11.4.4 Classes of Digital Signature Certificates

There are 4 general classes of Digital Signatures, classified as per the level of assurance.

- Class 0: Issued for demonstration / test purpose
- Class 1: Issued to individuals/ private subscribers. This class of subscriber will authenticate only the username and the e-mail id
- Class 2: Issued to both business persons and private individuals. This class of certificates confirms the information provided by the subscriber
- Class 3: Issued to individuals as well as organizations. This class of certificate is used in the e-Commerce application wherein high assurance of certificates is required. This certificate is issued to an individual only on their personal appearance before the CA

11.4.5 Electronic Signatures - IT Act Amendments

The PKI based Digital Signature Regime specified in the IT Act, 2000 is not Technology neutral and hence is against the recommendations of the UNCITRAL Model Law on Electronic Signatures, 2001. According to UNCITRAL, any electronic signature technology which fulfills the criteria of equivalence between handwritten and electronic signatures should be admissible, without prejudice to any particular Technology.

Accordingly, the IT Act Amendments of 2008 provided recognition to other electronic signature technologies, which are identified by the Central Government. The conditions to be fulfilled for the reliability of electronic signatures were laid down in the Amendments:

- The signature creation data or the authentication data are, within the context in which they are used, linked to the signatory or, as the case may be, the authenticator and to no other person;

- The signature creation data or the authentication data were, at the time of signing, under the control of the signatory or, as the case may be, the authenticator and of no other person;
- Any alteration to the electronic signature made after affixing such signature is detectable;
- Any alteration to the information made after its authentication by electronic signature is detectable; and
- It fulfils such other conditions which may be prescribed (in Rules)

The Central Government may, by notification in the Official Gazette, add to or omit any electronic signature or electronic authentication technique and the procedure for affixing such signature from the Second Schedule. The Central Government may prescribe the procedure for the purpose of ascertaining whether electronic signature is that of the person by whom it is purported to have been affixed or authenticated.

As on the current date, no electronic signature technique have been endorsed in Schedule II: Electronic Signature or Electronic Authentication Technique and Procedure

11.5 Cyber Crime Provisions in IT Act

11.5.1 Introduction to Cyber Crimes

Cyber crime or computer crime refers to any crime that involves a computer and a network, where the computers may or may not have played an instrumental part in the commission of a crime.

Some examples of cyber crimes:

- Virus attacks
- Stealing user credentials
- Credit card frauds
- Cyber pornography

In cyber crime cases, Computer may the role of weapon / target (credit card fraud), tool for the crime (denial of service attacks) or storage facility for the crime (pornography).

The knowledge of cyber crimes is essential for e-Governance personnel. In many e-Governance projects, contraventions to Cyber Security and Cyber Crime provisions are common:

- Sharing of passwords
- Sharing of Digital Signature Certificates
- Unintentional use of pirated software / making illegal copies of software
- Using government IT facilities for download of pirated music

In most cases, the contravention is done without understanding the legal implication and magnitude of the offense. Accordingly, Government personnel and Operators should be educated about the legal implications of contraventions and offense.

11.5.2 Cyber Crime provisions in the IT Act

A quick snapshot of the cyber crime provisions in the IT Act is given below:

Section 43: Civil Wrongs under IT Act

Certain Civil wrongs are defined in the IT Act, for which the offender shall be liable to pay damages by way of compensation not exceeding Rupees One crore to the affected party. The compensation is decided through an adjudication process. These offences include:

- Whoever without permission of owner of the computer
    - Secures access to the computer, computer system or network

  - Downloads, copies, extracts any data
  - Introduces or causes to be introduced any viruses or contaminant
  - Damages or causes to be damaged any computer resource
  - Destroy, alter, delete, add, modify or rearrange
  - Change the format of a file
  - Denies or causes denial of access to any authorized computer user
  - Disrupts or causes disruption of any computer resource

- Assists any person to do any thing above

  - Rogue Websites, Search Engines, Insiders providing vulnerabilities

- Charges the services availed by a person to the account of another person by tampering or manipulating any computer resource

  - Credit card frauds, Internet time thefts

Section 43A was added with Amendments of 2008 to make it mandatory for corporate bodies handling sensitive personal data (e.g. mail services, banks, insurance companies) to put in place security practices as prescribed by the Central government. Computer source code was also brought into ambit of civil wrongs by the amendments of 2008.

Section 65: Tampering with Source Code

Computer Source Code is the most important asset of software companies. "Computer Source Code" means the listing of programs, computer commands, design and layout. According to Section 65, if anyone knowingly or intentionally conceals, destroys or alters computer source code, when the computer source code required to be kept or maintained by law, it is punishable by fine up to Rs.2 lakh and / or imprisonment up to three years.

Section 66: Criminal Offenses

Section 66 was amended with the IT Act Amendments of 2008 to bring more crimes in its purview. The section is applicable to all contraventions listed in Section 43, when the offense is done "dishonestly" and "fraudulently", with penalties for such contraventions increased to Rs. 5 lakh. Certain new Sections were added to clarify and expand the scope of the Act:

- Section 66A: Sending offensive Messages - Applies to any information that is grossly offensive or menacing or false information. Also covers Cyber Stalking and Phishing.
- Section 66B: Receiving a Stolen Computer Resource - Applies to purchase or trading or use of stolen computers or mobiles besides information
- Section 66C: Identity Theft - Applies to Password theft, theft of cryptographic key etc
- Section 66D: Cheating by impersonation - Applies to Phishing, Job Frauds etc
- Section 66E: Violation of Privacy - Applies to Video Voyeurism
- Section 66F: Defines Cyber Terrorism and punishment for the same. Offenses under this section punishable with imprisonment which may extend to imprisonment for life
- Section 66F (A): Act done with the intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by:

  - denying or cause the denial of access to any person authorized to access computer resource; or
  - attempting to penetrate or access a computer resource without authorization or exceeding authorized access; or
  - introducing or causing to introduce any computer contaminant;

- 66F (B): Accessing computer resources that is restricted for reasons for the security of the State or foreign relations, with reasons to believe that such resources so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India

Section 66A in conjunction with the Indian Penal Code, is used for different criminal offenses, as listed below:

Scenario	Sections violated	Liable party
The passwords to an online bank account is stolen and fraudulent transfers made	Section 43 & 66 of IT Act, Section 420 IPC	Person who has stolen and misused the account details
Victim's e-mail account is hacked and used to send malicious content	Section 43 & 66 of IT Act	Person who has stolen and misused the account details
The contents of a music CD is Illegally ripped and sold online	Section 43 & 66 of IT Act, Section 63 of Copyright Act	The seller and buyer of the illegally copied music
Victim's e-mail hacked to extort money from victim threatening misuse of confidential information	Section 43 & 66 of IT Act, Section 384 of IPC	Person who has stolen and misused the account details

Section 67: Cyber Pornography

This crime involves publishing or transmitting or causing to be published obscene material in electronic form. Punishment on first conviction is imprisonment of either description up to 3 years and fine up to Rs 5 lakh. For subsequent conviction the punishment is imprisonment of either description up to 5 years and fine up to Rs.10 lakh.

11.5.3 Other Cyber Crime Related Provisions

The Act provides the authority to designated Government agencies to intercept, monitor or decrypt any information stored in a computer resource, in the cases concerning:

- Sovereignty or integrity of India,
- The security of the State,
- Friendly relations with foreign States,
- Public order or
- Preventing incitement for commission of a cognizable offence

The Act also provides Central government, the power to issue directions to block public access of any information to any computer resource, in cases stated in Section 69.

The Act (Section 79) provides for non liability of Intermediaries (e.g. ISPs, online auction portals like eBay) for any third party information, data or communication link made available by him, in certain cases:

- The role of the intermediary is limited to providing a communication system (as in an online auction system)
- Intermediary does not initiate the transmission, select the receiver, and select or modify any information in the transmission (as in the case of peer to peer sharing of pirated music)

Non liability does not apply:

- If the intermediary conspired or abetted in the unlawful act

- The intermediary fails to expeditiously remove or disable access to the material on that resource (without affecting the evidence to the unlawful act), on acquiring knowledge of the unlawful act or being notified by appropriate government agency on the act

The Act envisages the Cyber Appellate Tribunal as the appellate body for crimes under the IT Act, 2000 and its amendments.

11.6 Applicability of Other Legislations vis-a-vis IT Practices

11.6.1 Indian Penal Code & Indian Evidence Act

IT Act and its amendments does not cover all possible Cyber Crimes. Many Cyber Crimes come under the Indian Penal Code - with support from relevant provisions of the IT Act. A snapshot of such crimes covered under IPC is given below:

Crime	IPC Section
Sending threatening messages by email	Sec 503 IPC
Sending defamatory messages by email	Sec 499, 500 IPC
Forgery of electronic records	Sec 463, 470, 471 IPC
Bogus websites, cyber frauds	Sec 420 IPC
Email spoofing	Sec 416, 417, 463 IPC
Web - Jacking	Sec. 383 IPC
Criminal breach of trust / Fraud	Sec 405, 406, 408, 409 IPC
Destruction of electronic evidence	Sec 204, 477 IPC
False electronic evidence	Sec.193 IPC
Offences by or against public servant	Sec.167,172,173,175 IPC

First Schedule of IT Act, 2000 and Part III of IT Amendment Act, 2008 provides amendments to the IPC to incorporate electronic records.

The Indian Evidence Act, 1872 was amended to recognize electronic evidence, through Second Schedule of IT Act, 2000 and Part IV of IT Amendment Act, 2008:

- Section 3 of the Evidence Act amended to take care of admissibility of Electronic Records as evidence along with the paper based records as part of the documents which can be produced before the court for inspection.
- Section 47A: "When the Court has to form an opinion as to the digital signature of any person, the opinion of the Certifying Authority which has issued the Digital Signature Certificate is a relevant fact"
- Section 67B: Conditions to be fulfilled for admissibility of electronic records as evidence
- Section 73A: The verification of Digital Signature should either be by Controller of CAs or by any other person using the signer's public key

The amendments have paved the way for electronic evidence to be admissible in a court of law.

11.6.2 Intellectual Property Related Laws

Intellectual Property is all about Legal Rights to product of thought, creativity and intellectual effort. IPR Regime is put in place to incentivize innovation, creativity and research expenditure by facilitating the creator / inventor to have monopoly rights to monetize the output of his intellectual efforts. The subject matter of IPR is in many cases intangible: a logo or a trade mark, exhaust pipes for cars with a new design etc.

A robust IPR regime is essential for an economy to encourage and sustain innovation. There are different types of IPR protection available. The major IPR types having an impact in the e-

Governance / IT arena are Copyrights, Patents and Trademarks.

The Laws governing these IPR types are the following:

- Copyrights Act, 1957
- Patents Act, 1970
- Trademarks Act, 1999

11.6.3 Copyrights

A Copyright is an Exclusive Right to do or authorize others do certain acts in relation to:

- Original literary, dramatic, musical and artistic works
- Cinematograph film
- Sound recording

The Rights include the rights of reproduction, communication to the public, adaptation and translation of the work. Copyright exists in expression of an idea and it is not a right in the novelty of it. Its object is to protect the writer and author from the unlawful reproduction, plagiarism, piracy, copying and imitation. Violation of the copyright is confined to the form, manner, arrangement and expression of the idea by the author.

Copyrights are the primary source of protection for computer software in India. The Copyright Act treats Computer Software as a special case of "literary work" extends the same protection as applies to other literary works. Copyright protection makes it illegal to make or distribute copies of copyrighted software without proper or specific authorization (Section 16 of Copyright Act).

Copyright protection assumes significance in the e-Governance context. If a third party Software Vendor is commissioned to develop Software, the Copyright for the software does not automatically vest with the commissioning authority, but with the Vendor. In case the commissioning party intends to obtain the Copyright to the Software, it has to be done through a formal written deed of assignment. To overcome this limitation, Copyright / IPR assignment should be formally drafted into the Contract between the Vendor and the Department.

Copyright protection is confined to only to form and expression and not to the underlying idea - thus protection is only against Software piracy. In Software products, the creative idea behind the Software may be a more important Intellectual Property than just the source code in many cases. This is necessarily true for innovations in Software, for which the Owner invests substantial amount of money. Such innovations are provided extra protection by patents.

11.6.4 Patents

A patent is an exclusive right granted by a country to the owner of an invention to make, use, manufacture and market the invention, provided the invention satisfies certain conditions stipulated in the law. Patents are governed by the Indian Patents Act of 1970 and The Patents Rules 2003 and amendments thereof.

For applying for a patent, the invention should satisfy certain criteria:

- Novelty
- Inventive Step or non-obviousness
- Utility or Industrial Application

During this period (20 years), the inventor is entitled to exclude anyone else from commercially exploiting his invention.

Computer Software in not yet covered under the patents regime in India, except for certain sub set of computer software including embedded software (those software having industrial application).

11.6.5 Trademarks

Trademarks are governed in India by the Trademarks Act, 1999, which is in accordance with the TRIPS (Trade Related aspects of Intellectual Property Rights) Agreement, of which India is a signatory.

"A trademark is a distinctive sign or indicator used by an individual, business organization, or other legal entity to identify that the products or services to consumers with which the trademark appears originate from a unique source, and to distinguish its products or services from those of other entities"

In the Cyber World, Trademark Regulations has implications in the allotment of domain names. Domain names are website addresses (e.g. www.nisg.org) which map to a particular IP address (e.g. 64.208.159.11). By using a domain name which is similar to the trademark of another entity, misunderstanding can be created in the minds of general public on the identity of that trademark, resulting in trademark infringement.

But a domain name is not itself a trademark, but only an expression of a trademark. A domain name is a word or phrase registered in the domain name registration system. Whether a word or phrase used in a domain name qualifies for trademark protection is determined under regular trademark law.

In India, the domain names which end in ".in" are governed by the .IN Registry set up by DIT.
The disputes regarding domain names in the ".in" domain are resolved in the following manner:

- A Trademark holder (complainant) can file a complaint with the .IN Registry against a person who has registered a domain name (registrant), on any of the following grounds:
    - the Registrant's domain name is identical or confusingly similar to a name, trademark or service mark in which the Complainant has rights,
    - the Registrant has no rights or legitimate interests to the domain name,
    - the Registrant's domain name has been registered or is being used in bad faith
- The Complainant can ask for any of the following remedies:
    - Cancellation of Registrant's domain name
    - Transfer of domain name to the complainant
- The .IN Registry appoints an arbitrator, who gives his decision based on Arbitration and Conciliation Act 1996 and the IDRP (.IN Domain Dispute Resolution Policy) and Rules

The various types of domain name related offenses are the following:

- Cyber squatting is the registration of a domain name by someone who lacks a legitimate claim with the intent to sell the name, or to prevent the trademark holder from gaining access to the name, or to divert traffic : e.g. www.whitehouse.com / www.whitehouse.org case
- Typo squatting is the case in which the squatter registers a variant of a famous trademark : e.g. www.google.com

Though many other countries have separate cyber squatting laws, such cases are handled in India under the provisions of the Trademarks Act.

11.7 Other Legal Aspects

11.7.1 Portals in e-Governance projects and Legal Implications

Portals are used widely in e-Governance for web enablement of citizen (G2C) and Business (G2B) services. Portals help achieve the following e-Governance goals:

- Converting department services (rendered at department premises) to self services (rendered online)
- Anywhere / anytime delivery of government services
- Providing information services of the department

Use of Portals for government service delivery gives rise to many legal considerations, which should be addressed adequately in order to build trust and confidence in the government portal. Such Legal considerations for portal based service delivery are addressed through a set of policies and terms & conditions drafted for each portal:

- Portal Terms & Conditions
- Privacy Policy
- Copyright statement / policy
- Hyper linking Policy

There are certain general principles based on which these policies are prepared for each e-Government portal. These principles are discussed below:

11.7.2 Portal Terms & Conditions

The Portal Terms & Conditions should have clearly defined Terms & Conditions addressing the following aspects related to portal use:

- Portal ownership details: Who owns the portal
- Usage policy of content:
  - The rules and regulations governing the usage of the content provided in the portal and the transaction services extended by the portal
  - Specific contractual clauses for system usage (e.g: Submission of false information leads to cancellation of registration or blacklisting (e.g. e-Procurement, MCA21)
- Legal aspects: Governing law, and which court of law will have jurisdiction in case of legal disputes arising out of the portal content
- Disclaimers: Disclaiming the contents linked from a non-government website
- Liability and Indemnity: Limitation of Liability for government
- Responsibility towards hyperlinked sites

The Terms & Conditions should be presented to the citizen / business entity (portal user) while registering for use of portal. Only after agreeing to the Portal Terms & Conditions, should be user be allowed access to the services rendered through the portal

The Terms & Conditions presented by the portal and agreed to by the portal user, constitute a valid legal contract between the user and the government (portal owner), as per the provisions of:

- Clauses of Indian Contract Act, 1872 (pre-requisites for a contract)
- Section 1OA of IT Act (contract formation and other pre-requisites of a contract can be fulfilled through electronic means)

Accordingly the Terms & Conditions have the validity of a legal contract in the court of law in case of legal disputes arising out of portal usage.

11.7.3 Privacy Policy

Most portals collect personal details / information from users, either during Portal Registration or during the course of delivery of services (e.g. income tax). Only that information which is absolutely essential for service delivery should be collected by the Portal.

Portals should have a Privacy Policy, which clearly states:

- The purpose for which the personal data is collected
- Whether the data shall be disclosed to anyone - to whom and for what purpose
- In case the portal handles high risk personal information (credit card, bank details etc), the safeguards should be mentioned (SSL, Digital Certificates etc)
- Whether cookies (software downloads which collect user's personal data) will be transferred to visitor's system, and what is their purpose

The Privacy Policy should be prominently displayed on the Portal and the Portal Terms & Conditions should refer to the Privacy Policy.

11.7.4 Content Copyright

All content provided in the portal should be backed up with proper Copyright Policy, explaining the terms and conditions of their usage and reference by others. The copyright policy of the department may be liberal, moderate or conservative

- Liberal / moderate: Allows reproduction of content without prior permission.
- Acknowledgement of source is to be provided in case of reproduction. safeguards against derogatory use of content.
- Content can be reproduced only after prior permission. Specific limitations for use of content.

In case of content having third party copyright, all prior permissions should be obtained before publishing in the government portal.

11.7.5 Hyper-linking Policy

Any other website (external or government) hyperlinked at the government portal may be viewed by users as having the stamp of approval and confidence of the government. In many cases, external websites may provide links to the government portals. Therefore, all government portals should have clear-cut Hyper linking policy which spells out the criteria and guidelines for providing hyperlinks to external sites

In case of other sites providing hyperlinks to government portal:

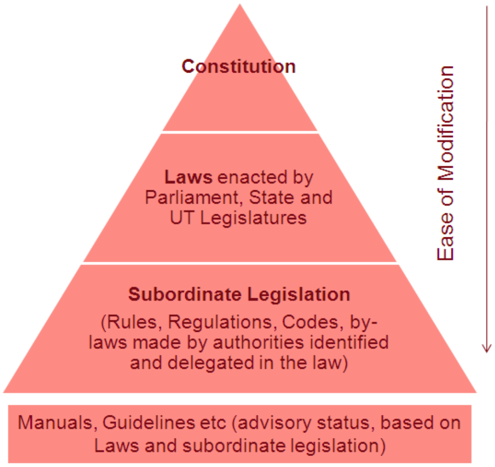
- The policy should clearly state whether the external site will have to take prior permission for providing hyperlinks
- Policy should specify that the hyperlink should open up the government portal in a new browser page (instead of in a frame within the external site)

In case of providing hyperlinks to other government / non-government sites in the portal:

- The policy should lay down the specific guidelines / criteria for deciding which external websites can be linked from the portal
- If non-government websites are linked there should be a strong business rationale for the same (e.g. providing link to the site of Licensed CA in e-Procurement / Income Tax portal)
- Whenever the user moves to another portal through a hyperlink, an indication shall be provided to the user on the same

11.7.6 Domain Legislation

In any e-Governance initiative, it is important to back it up with the required legal changes in the legislation in the domain. Processes are usually derived from the underlying legislation. Many e-Governance initiatives require changes to processes, institutional structures etc. Such changes may require change to the legal framework, to legalize the process changes, and give them enough legal backing. To understand domain legislations, consider the hierarchy of legislation given below:


Constitution
Laws enacted by Parliament, State and UT Legislatures
Subordinate Legislation
(Rules, Regulations, Codes, by-laws made by authorities identified and delegated in the law)
Manuals, Guidelines etc (advisory status, based on Laws and subordinate legislation)
Ease of Modification

At the top of the Legal hierarchy is the Constitution. Laws are enacted by Central or State government depending on whether State / Central subject.

Subordinate legislation enacted by authorities identified under the law. At the lowest level are the manuals and guidelines, which have only advisory status.

While the laws need ratification by the Parliament / State / UT Legislatures, Subordinate legislation can be amended by executive orders. Accordingly, the practice followed in legislation is to delegate the procedural issues to subordinate legislations, while the Laws provide only a high level direction.

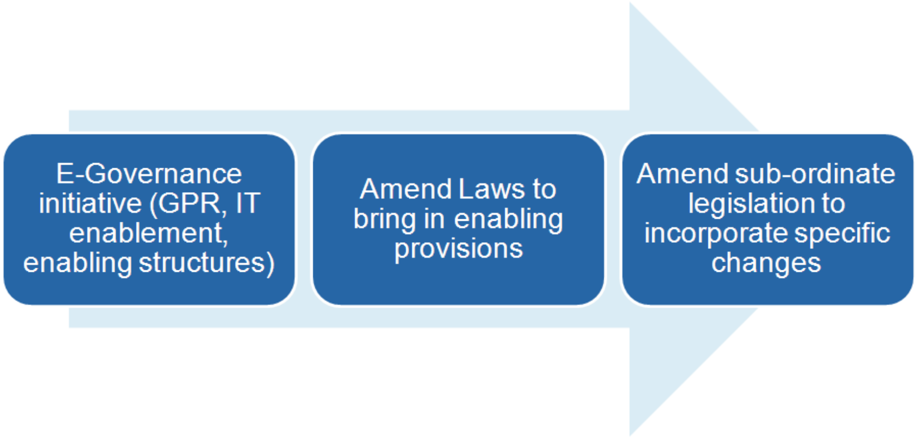
To illustrate an example of domain legislation, the example of MCA21 may be considered. MCA21 was rolled out to enable electronic filing of compliance information by companies. The processes of Company Registration and Compliance filing were based on the Companies Act, 1956 (and the Rules made there-under) and the Monopolies and Restrictive Trade Practices Act 1969.

In order to provide legal backing to the initiative, necessary changes were made to the Companies Act:

- Amendments to mandate Director Identification Number
- Insertion of provisions 610B to 610E to mandate electronic filing

Though most of the e-Governance projects may not require changes to domain legislation, projects with a Government Process Re-engineering component requires legal changes. This is because some of the changes that may result from GPR will requires legal changes:

- Organizational Structures change (e.g. change in designated agency to handle a particular task / process)
- Jurisdictions change (anytime / anywhere services)
- Statutory powers change (who is the authority for delivery of a certain service) The approach to incorporate changes to the domain legislation is given below:


E-Governance initiative (GPR, IT enablement, enabling structures)
Amend Laws to bring in enabling provisions
Amend sub-ordinate legislation to incorporate specific changes

It is a good practice to conduct Legal compliance audit in large e-Governance projects to ensure the following legal requirements are fulfilled:

- The project is in compliance with the Legal and Regulatory framework (IT Act, Public
- Records Act, Other domain legislation etc)
- Any changes in the domain laws necessitated by the e-Governance initiative (change in processes, institutional structures, statutory powers etc) are addressed appropriately
- Sufficient legal backing is available to government, in case of disputes that may arise

11.8 Regulatory Framework under NeGP

National e-Governance Plan (NeGP) provides a holistic approach and direction for e-Governance Implementation across the country. It follows a program based approach to gain momentum across the various arms and levels of Government guided by a common vision, strategy and approach. The Plan was formulated by the Department of Information Technology (DIT) and Department of Administrative Reforms & Public Grievances (DAR&PG), and approved by the Union Government in May, 2006.

NeGP implementation poses many challenges:

- Centralized initiative, decentralized implementation
    - Implementation of State MMPs are handled by each state individually with support from the Central government
    - Successful implementation in one state can be easily replicated in another, as underlying processes are similar (e.g. Land Records, Property Registration)
- Different systems will need to interact with each other : e.g. Registration system and Land Records system
- Aggregation of data across the country from systems : e.g. CCTNS, NCRB, SSDG

To overcome these challenges, NeGP has set out certain Guidelines to ensure Standards and Interoperability is ensured.

The Framework of Standards under NeGP includes the following:

- National Policy on Open Standards
- Localization and Language Technology Standards

  - Character Encoding Standards
  - Font Standards

- Metadata and Data Standards
- Quality Assurance and Conformance Standards
- Network and Information Security Standards
- Framework of Policies and Guidelines for Common Infrastructure MMPs
  - SDC guidelines
  - SWAN Guidelines
  - CSC policies
- .IN Domain name policies
- Implementation guidelines for other Mission Mode Projects

Though the policies under NeGP have only advisory status, they are important from the point of view of ensuring Standards and Interoperability.

National Policy on Open Standards

The national policy on Open Standards was set out by DIT, with the following purpose:

- Sets out guidelines for the consistent, standardized and reliable implementation of e-Governance solutions.
- Ensure seamless interoperability of various e-Governance solutions developed by multiple agencies.
- Improve the technology choices available and avoid vendor lock-in

The policy is applicable for all systems used in e-Governance, and all standards used in e-Governance systems, including interfaces and data archival. All legacy systems should ensure external interfaces adhere to the policy.

The policy envisages selection of a single standard in each technical domain, which complies with certain mandatory and desirable characteristics. The mechanism for finalizing and implementing the standards is given below:

- GoI identifies domains for standardization and identifies the authorized agency to select the standard
- The selected agency shortlists the standards and after extensive consultations, finalizes the standard
- Once standard is recommended, industry shall be given a definite time for progressive compliance with the standards, be it for interface or for the entire system.

Once the standard is finalized, all Government IT Systems should comply with the standard recommended in the particular domain. All Requests for Proposals for e-Governance systems shall include the guidelines for ensuring compliance to Open Standards.

12. Information Security issues in e-Governance

The rise of e-government has been one of the most striking developments of the web. As the Internet supported digital communities evolve, and assuming that they do indeed grow to incorporate individuals around the country, they present the government with a number of challenges and opportunities. In an e-Government project, a substantial amount of documentation is done like maintenance of land records, police records and so on. Each department is critical so that only authorized people get into the network and access the information. An understanding of the information security technology and the need for its implementation is key for safer, secured and smooth functioning of e-governance undertaking.

12.1 Introduction

Any e-governance initiative will remain venerable to security breaches in absence of a well articulated security policy. Information Security Policies are the cornerstone of information security effectiveness. The Security Policy is intended to define what is expected from an organization with respect to security of Information Systems. The overall objective is to control or guide human behavior in an attempt to reduce the risk to information assets by accidental or deliberate actions. Information security policies underpin the security and well being of information resources. They are the foundation, the bottom line, of information security within an organization. In an organization, having the right information at the right time can make the difference between success, and failure. Data Security will help the user to control and secure information from, inadvertent or malicious changes and deletions or unauthorized disclosure. There are three aspects of data security:

- **Confidentiality:** refers to protection of information from unauthorized disclosure e.g. to the press or to release through improper disposal techniques, or to those who are not entitled to have the same.
- **Integrity:** is about protecting information from unauthorized modification, and ensuring that information, such as a beneficiary list, can be relied upon and is accurate and complete.
- **Availability:** is to ensure that the information is available when it is required.

Thus, three basic security concepts, important to information on the Internet are confidentiality, integrity, and availability. When information is read or copied by someone not authorized to do so, the result is known as loss of confidentiality. For some types of information, confidentiality is a very important attribute. Examples include research data, medical and insurance records and government investment strategies. In some locations, there may be a legal obligation to protect the privacy of individuals. This is particularly true for banks and loan companies; debt collectors; businesses that extend credit to their customers or issue credit cards; hospitals, doctors' offices, and medical testing laboratories; individuals or agencies that offer services such as psychological counseling or drug treatment; and agencies that collect taxes. Information can be corrupted when it is available on an insecure network.

When information is modified in unexpected ways, the result is known as loss of integrity. This means that unauthorized changes are made to information, whether by human error or intentional tampering. Integrity is particularly important for critical safety and financial data used for activities such as electronic funds transfers, air traffic control, and financial accounting. Information can be erased or become inaccessible, resulting in loss of availability. When a user cannot get access to the network or specific services provided on the network, they experience a denial of service.

To make information available to those who need it and who can be trusted with it, organizations use authentication and authorization. Thus, concepts relating to the people who use that information are authentication, authorization and non-repudiation. Authentication is proving that a user is whom he or she claims to be. That proof may involve something the user knows (such as a password), something the user has (such as a "smartcard" or something about the user that proves the person's identity (such as a fingerprint). Authorization is the act of determining whether a particular user (or computer system) has the right to carry out a certain activity, such as reading a file or running a program. Security is strong when the means of authentication cannot later be refuted - the user cannot later deny that he or she performed the activity. This is known as non-repudiation. A network security incident is any network-related activity with negative security implications. This usually means that the activity violates an explicit or implicit security policy.

12.2 Information Security Threats

Incidents come in all shapes and sizes. They can come from anywhere on the Internet, although some attacks must be launched from specific systems or networks and some require access to special accounts. A cyber attack [2] may be a comparatively minor event involving a single site or a major event in which tens of thousands of sites are compromised. A typical attack pattern consists of gaining access to a user's account, gaining privileged access, and using the victim's system as a launch platform for attacks on other sites. It is possible to accomplish all these steps manually in as little as 45 seconds; with automation, the time decreases further. Though, it is difficult to characterize the people who cause incidents. An intruder may be an adolescent who is curious about what he or she can do on the Internet, a college student who has created a new software tool, an individual seeking personal gain, or a paid "spy" seeking information for the economic advantage of a corporation or foreign country. An incident may also be caused by a disgruntled former employee or a consultant who gained network information while working with a company. An intruder may seek entertainment, intellectual challenge, a sense of power, political attention, or financial gain. Thus, the networks providing data to the end users of the e-Government remain vulnerable to variety of threats such as packet sniffing, probing etc.

A) Packet Sniffer

A packet sniffer, sometimes referred to as a network monitor or network analyzer, can be used legitimately by a network or system administrator to monitor and troubleshoot network traffic. Using the information captured by the packet sniffer an administrator can identify erroneous packets and use the data to pinpoint bottlenecks and help maintain efficient network data transmission. An unauthorized packet sniffing, however, can lead to serious breaches in electronic business and secured transmission.

B) Probe

Probe is a class of attacks where an attacker scans a network to gather information or find known vulnerabilities. An attacker with map of machine and services that are available on a network can use the information to notice for exploit e.g. ipsweep, portsweep, nmap, satan.

C) Malware

Malware, short for malicious software, consists of programming (code, scripts, active content, and other software) designed to disrupt or deny operation, gather information that leads to loss of privacy or exploitation, gain unauthorized access to system resources, and other abusive behavior. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code. Malware is a general term for programs that, when executed, would cause undesired results on a system. Users of the system usually are not aware of the program until they discover the damage. Malware includes Trojan horses, viruses, and worms. Trojan horses and viruses are usually hidden in legitimate programs or files that attackers have altered to do more than what is expected. Worms are self replicating programs that spread with no human intervention after they are started. Viruses are also self-replicating programs, but usually require some action on the part of the user to spread inadvertently to other programs or systems. These sorts of programs can lead to serious data loss, downtime, denial of service, and other types of security incidents.

D) Internet infrastructure attacks

These rare but serious attacks involve key components of the Internet infrastructure rather than specific systems on the Internet. Examples are network name servers, network access providers, and large archive sites on which many users depend. Widespread automated attacks can also threaten the infrastructure. Infrastructure attacks affect a large portion of the Internet and can seriously hinder the day-to-day operation of many sites.

E) Denial of Service (DOS) attack

A denial of service attack is a class of attacks where an attacker makes a computing or memory resource too busy or too full to handle legitimate requests, thus denying legitimate user access to a machine e.g. neptune, teardrop, smurf, pod, back, land. Attackers may "flood" a network with large volumes of data or deliberately consume a scarce or limited resource, such as process control blocks or pending network connections. They may also disrupt physical components of the network or manipulate data in transit, including encrypted data. Exploitation of Trust Computers on networks often has trust relationships with one another. For example, before executing some commands, the computer checks a set of files that specify which other computers on the network are permitted to use those commands. If attackers can forge their identity, appearing to be using the trusted computer, they may be able to gain unauthorized access to other computers.

F) Remote to Local (R2L) attack

A remote to local attack is class of attacks where an attacker sends packets to a machine over network, then exploits the machine's vulnerability to illegally gain local access to a machine e.g. guss_passwd, ftp_write, multihop, imap, phf, spy, warezmaster, warezclient. An account compromise is the unauthorized use of a computer account by someone other than the account owner, without involving system-level or root-level privileges. An account compromise might expose the victim to serious data loss, data theft, or theft of services.

G) User to root (U2R) attack

User to root (U2R) attacks are a class of attacks where an attacker starts with access to a normal user account on the system and is able to exploit vulnerability to gain root access to the system e.g. loadmodule, perl, buffer_overflow, rootkit. A root compromise is similar to an account compromise, except that the account that has been compromised has special privileges on the system. The term root is derived from an account on UNIX systems that typically has unlimited, or "superuser" privileges. Intruders who succeed in a root compromise can do just about anything on the victim's system, including run their own programs; change how the system works, and hide traces of their intrusion.

12.3 Improving Security in e-Governance

To make information available to those who need it and who can be trusted with it, a robust defense requires a flexible strategy that allows adaptation to the changing environment, well-defined policies and procedures, the use of robust tools, and constant vigilance. It is helpful to begin a security improvement program by determining the current state of security at the site. Methods for making this determination in a reliable way are becoming available. Integral to a security program are documented policies and procedures, and technology that support their implementation.

A) Security policy

If it is important to be secure, then it is important to be sure. All of the security policy is enforced by mechanisms that are strong enough. There are organized methodologies and risk assessment strategies to assure completeness of security policies and assure that they are completely enforced. In complex systems, such as information systems, policies can be decomposed into sub-policies to facilitate the allocation of security mechanisms to enforce sub-policies. A policy is a documented high-level plan for organization-wide computer and information security. It provides a framework for making specific decisions, such as which defense mechanisms to use and how to configure services, and is the basis for developing secure programming guidelines and procedures for users and system administrators to follow. Because a security policy is a long-term document, the contents avoid technology-specific issues.

- Definition of acceptable use for users
- Guidelines for reacting to a site compromise.
- High-level description of die technical environment of the site, the legal environment (governing laws), the authority of the policy, and the basic philosophy to be used when interpreting the policy
- Risk analysis that identifies the site's assets, the threats that exist against those assets, and the costs of asset loss
- Guidelines for system administrators on how to manage systems

B) Security Practices

The daily barrage of spam, now infested with zero-day malware attacks, not to mention the risks of malicious insiders, infected laptops coming and going behind the packet-inspecting firewalls and cyber attacks-prevention systems is the fact of networked communication today. This establishes need for steps of due care and due diligence towards a regulatory compliance, which must be put in place for smooth operations, if not in existence already.

System administration practices play a key role in network security. Checklists and general advice on good security practices are readily available. Below are examples of commonly recommended practices:

- Ensure all accounts have a password and that the passwords are difficult to guess. A one-time password system is preferable.
- Use tools such as MD5 checksums (8, a strong cryptographic technique, to ensure the integrity of system software on a regular basis.
- Use secure programming techniques when writing software. These can be found at security-related sites on the World Wide Web.
- Be vigilant in network use and configuration, making changes as vulnerabilities become known.
- Regularly check with vendors for the latest available fixes and keep systems current with upgrades and patches. Regularly check on-line security archives, such as those maintained by incident response teams, for security alerts and technical advice.
- Audit systems and networks, and regularly check logs. Many sites that suffer computer security incidents report that insufficient audit data is collected, so detecting and tracing an cyber attacks is difficult

Best practices are things done - steps taken - actions and plans carried out. For example, encryption is a best practice and not a product or tool. There are many commercially and freely available tools which may prove to be most suited for a best-practice model.

C) Security Procedures

Procedures are specific steps to follow that are based on the computer security policy. Procedures address such topics as retrieving programs from the network, connecting to the site's system from home or while traveling, using encryption, authentication for issuing accounts, configuration, and monitoring.

12.4 Security Technology

A variety of technologies [6] have been developed to help organizations secure their systems and information against intruders. These technologies help protect systems and information against attacks, detect unusual or suspicious activities, and respond to events that affect Security.

A) Operational Technology

Intruders actively seek ways to access networks and hosts. Armed with knowledge about specific vulnerabilities, social engineering techniques, and tools to automate information gathering and systems infiltration, intruders can often gain entry into systems with disconcerting ease. System administrators face the dilemma of maximizing the availability of system services to valid users while minimizing the susceptibility of complex network infrastructures to attack. Unfortunately, services often depend on the same characteristics of systems and network protocols that make them susceptible to compromise by intruders. In response, technologies have evolved to reduce the impact of such threats. No single technology addresses all the problems. Nevertheless, organizations can significantly improve their resistance to attack by carefully preparing and strategically deploying personnel and operational technologies. Data resources and assets can be protected, suspicious activity can be detected and assessed, and appropriate responses can be made to security events as they occur.

B) One-Time Passwords

Intruders often install packet sniffers to capture passwords as they traverse networks during remote log in processes. Therefore, all passwords should at least be encrypted as they traverse networks. A better solution is to use one-time passwords because there are times when a password is required to initiate a connection before confidentiality can be protected. One common example occurs in remote dial-up connections. Remote users, such as those traveling on business, dial in to their organization's modem pool to access network and data resources. To identify and authenticate themselves to the dial-up server, they must enter a user ID and password. Because this initial exchange between the user and server may be monitored by intruders, it is essential that the passwords arc not reusable. In other words, intruders should not be able to gain access by masquerading as a legitimate user using a password they have captured.

C) Cryptography

Sometimes it becomes necessary to encrypt the message sent, with the goal of preventing any one who is eavesdropping on the channel from being able to read the contents of the messages. One of the primary reasons that intruders can be successful is that most of the information they acquire from a system is in a form that they can read and comprehend. As millions of electronic messages that traverse the Internet each day, it is easy to see how a well- placed network sniffer might capture a wealth of information that users would not like to have disclosed to unintended readers. Intruders may reveal the information to others, modify it to misrepresent an individual or organization, or use it to launch an attack. One solution to this problem is, through the use of cryptography, to prevent intruders from being able to use the information that they capture.

Encryption is the process of translating information from its original form (called plain text) into an encoded, incomprehensible form (called cipher text). Decryption refers to the process of taking cipher text and translating it back into plaintext. Any type of data may be encrypted, including digitized images and sounds. The authenticity of data can be protected in a similar way. For example, to transmit information to a colleague by E-mail, the sender first encrypts the information to protect its confidentiality and then attaches an encrypted digital signature to the message. When the colleague receives the message, he or she checks the origin of the message by using a key to verify the sender's digital signature and decrypts the information using the corresponding decryption key. To protect against the chance of intruders modifying or forging the information in transit, digital signatures are formed by encrypting a combination of a checksum of the information and the author's unique private key. A side effect of such authentication is the concept of non-repudiation. A person who places their cryptographic digital signature on an electronic document cannot later claim that they did not sign it, since in theory they are the only one who could have created the correct signature.

D) Firewalls

A firewall is a set of related programs, located at a network gateway server that protects the resources of a private network from users from other networks. (The term also implies the security policy that is used with the programs.) An enterprise with an intranet that allows its workers access to the wider Internet installs a firewall to prevent outsiders from accessing its own private data resources and for controlling what outside resources its own users have access to. Its purpose is to eliminate from the stream those packets or requests that fail to meet the security criteria established by the organization. A simple firewall may consist of a filtering router, configured to discard packets that arrive from unauthorized addresses or that represent attempts to connect to unauthorized service ports. More sophisticated implementations may include bastion hosts, on which proxy mechanisms operate on behalf of services. These mechanisms authenticate requests, verify their form and content, and relay approved service requests to the appropriate service hosts. Because firewalls are typically the first line of defense against intruders, their configuration must be carefully implemented and tested before connections are established between internal networks and the Internet.

E) Analysis tools

There is strong need for analysis tool because of the increasing sophistication of intruder methods and the vulnerabilities present in commonly used applications, it is essential to assess periodically network susceptibility to compromise. A variety of vulnerability identification tools are available, which have garnered both praise and criticism. System administrators find these tools useful in identifying weaknesses in their systems. Critics argue that such tools, especially those freely available to the Internet community, pose a threat if acquired and misused by intruders.

F) Monitoring tools

Continuous monitoring of network activity is required if a site is to maintain confidence in the security of its network and data resources. Network monitors may be installed at strategic locations to collect and examine information continuously that may indicate suspicious activity. It is possible to have automatic notifications alert system administrators when the monitor detects anomalous readings, such as a burst of activity that may indicate a denial-of-service attempt.

Such notifications may use a variety of channels, including electronic mail and mobile paging. Sophisticated systems capable of reacting to questionable network activity may be implemented to disconnect and block suspect connections, limit or disable affected services, isolate affected systems, and collect evidence for subsequent analysis.

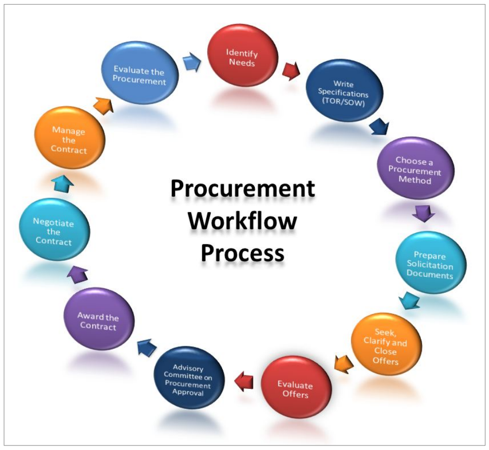
Understanding of security issues and developing a security perception based on perceived threat profile is important to articulation of a security policy. To translate policy in to a program of action and development of security infrastructure in line with the development of overall IT infrastructure has to be an integral part of e-governance enterprise architecture. The issues underlined and cost benefit tradeoffs have to be analyzed while proposing and implementing a solution.

12.5 Summary

It is evident from above that information security in an essential part of any e-governance initiative. In Indian e-governance scenario, however, the security aspects are not being taken as seriously. In large number of cases it is not difficult to see that the decision-makers in the government prefer to compromise when it comes to high- end technology adoption, implementation and maintenance. Digital security is critical in e-governance initiatives. Confidentiality of any transaction or information available on the network is crucial. The government document and other important material have to be protected from unauthorized users in case of e-governance projects. Hence security is critical for successful implementation of such projects. E-governance coupled with security systems providing adequate protection is the requirement of any system design effort to beat the inertia.

13. Procurement in e-Governance

13.1 Introduction to Government Procurement


Procurement Workflow Process
Identify Needs
Write Specifications (TOR/SOW)
Choose a Procurement Method
Prepare Solicitation Documents
Seek, Clarify and Close Offers
Evaluate Offers
Advisory Committee on Procurement Approval
Award the Contract
Negotiate the Contract
Manage the Contract
Evaluate the Procurement

Government procures goods, works and services which are incidental to government functioning and delivery of the services to citizens. Accordingly, government procures a large range of items
- from procuring civil works for road construction, health supplies for hospitals, services of IT providers etc. Public Procurement operates on the backbone of a broad framework of National laws dealing with relevant aspects of procurement. These laws include:

- Indian Contract Act, 1872;
- Sale of Goods Act, 1930;
- Companies Act, 1956;
- Arbitration & Conciliation Act, 1996;
- Limitation Act, 1963;
- Right to Information Act, 2005

Public Procurement in India is a State subject, and thereby the Regulatory Framework governing Public Procurement varies from State to State. 'General Financial Rules' (GFR), framed by the central financial ministry acts as the guideline for public procurement, but has only subordinate legislation status.

Various states have adopted their own Legal framework, based on the GFR and other best practices. Procurement funded by external donors (World Bank, ADB etc) follows guidelines by the donor in this regard

Government procurement is based on certain key principles. These include:

- Ensuring Transparency & Accountability in Public Procurement
- Achieving Best Value for Money for the government through efficient procurement and informed management
- Equal Opportunity to all qualified firms in participating in procurement opportunities and non discrimination
- Development of indigenous / Local industries (SSI Units)

In this section, we look specifically at the procurement of goods and services in e-Governance projects.

13.2 Procurement in e-Governance Projects

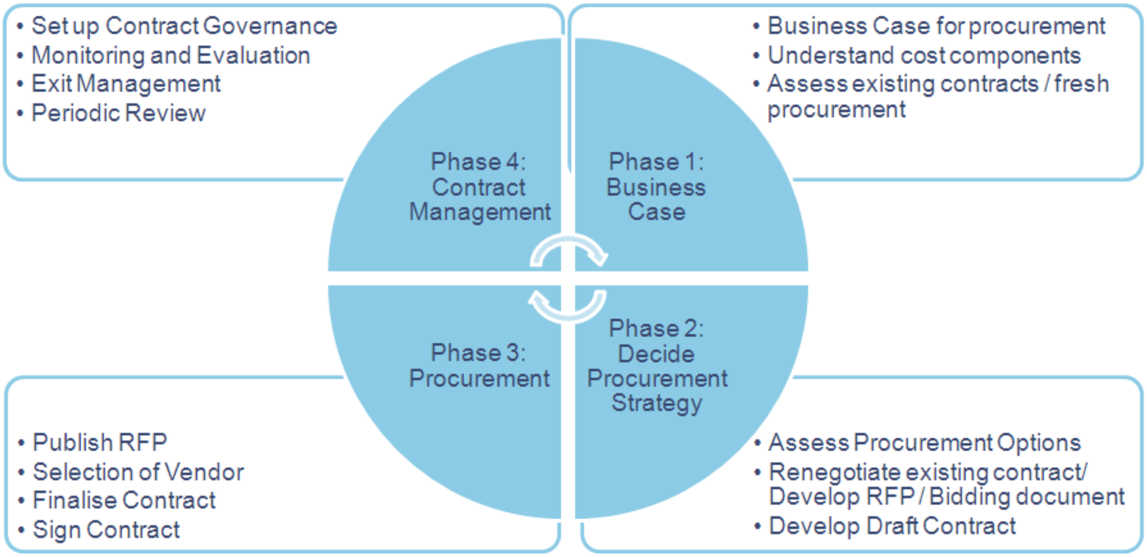
Procurement in e-Governance projects majorly involves procurement of Information systems. Procurement of IS poses many unique challenges. Information Systems are highly affected by changing business objectives, organizational politics, and institutional capacity of the end-user. They are subject to rapid technological change over the project lifecycle, and also entail mixtures of professional engineering services and supply of diverse hard and soft technologies. In many cases, their technical content is diverse and difficult to define.

Procurement in e-Governance projects are even more challenging, due to the following aspects:

- Projects range from straightforward Supply and Installation of products to complex development, integration and operation of mission-critical Information Systems

- Varied Business Models including Public Private Partnership

The various stages in the procurement Lifecycle in e-Governance projects are indicated in the figure below:


• Set up Contract Governance
• Monitoring and Evaluation
• Exit Management
• Periodic Review
• Business Case for procurement
• Understand cost components
• Assess existing contracts / fresh procurement
Phase 4: Contract Management
Phase 1: Business Case
Phase 3: Procurement
Phase 2: Decide Procurement Strategy
• Publish RFP
• Selection of Vendor
• Finalise Contract
• Sign Contract
• Assess Procurement Options
• Renegotiate existing contract/ Develop RFP / Bidding document
• Develop Draft Contract

During the Business Case phase, the justification for undertaking the project and its feasibility are explored. The Business Case phase includes the following activities, which usually results in a Feasibility Study Report and Detailed Project Report (DPR):

- Defining Objectives, Vision and Mission for the initiative
- Study of Best Practices from similar contexts
- Stakeholder Consultations
- Understand cost components for the project
- Detailed analysis of business case
- Business justification for the project (better service levels)
- Cost Benefit Analysis
- Analysis of risks and mitigation measures

In case of transition from existing system / vendor, the analysis of benefits of continuing with the current arrangement vs. fresh procurement is carried out

13.3 Deciding on Procurement Strategy

The first step in deciding Procurement Strategy is to identify and segregate the project components. An indicative list of components that can come up in an e-Governance project is given below:

- **ICT Strategy and Consultancy:** ICT strategy, defining ICT architecture, ICT security, RFP preparation for ICT vendor and procurement, contract management, and training
- **Applications development / Software implementation:** Custom applications development, deployment of COTS products, Project Management
- **Deployment IT Infrastructure:** Hosting infrastructure and storage, distributed infrastructure and LAN servers (desktop, laptops, printers, software licenses, local servers)
- **Operations and Maintenance:** Operations management (operations administration, database management etc.), service delivery, helpdesk support, facilities management.
- Communications: Communications infrastructure (network connectivity, PABX,

videoconferencing, etc.), voice (fixed and mobile), and data/ISP

In this step the components are logically grouped together and decision is taken on whether they can be self managed or outsourced. Components which are covered by Infrastructure / Resources already available components for which departments can build the required internal resources, and which requires strategic control shall be self managed.

The opportunities for bundling outsourced components are identified, based on the interrelation between the components and department context. Based on the components to be outsourced, department can go in for single or multiple vendors.

The implications of having single vendor are:

- Optimum option if all the components for external sourcing can be bundled into one group
- Suited for smaller agencies and agencies in which ICT is not highly strategic or customized
- Subcontracting and Consortium arrangements may be used to bring in diverse capabilities with one single entity taking overall responsibility
- More cost effective than managing multiple vendors
- The implications of having multiple vendors are:
- Better suited for large agencies with highly specific and strategic ICT functions
- Provides greater control over vendor performance
- Requires higher capacities in the department and higher coordination risk
- Allows for best of the breed solutions in each component
- Identify opportunities for bundling outsourced components: One or Multiple outsourcing vendors

13.4 Planning the Procurement

Based on the Procurement context, any of the following procurement modes may be employed:

- **Two stage competitive process:** Expression of Interest, followed by Request for Proposal open to bidders qualified from EoI process
- **Single stage competitive process:** Request for Proposal open to all bidders fulfilling the qualifying criteria
- **Request for Quotes:** Used for standardized requirements, in which price is the only deciding factor
- **Procurement from Rate Contracts:** For items with standard specification, for which Rates have already been negotiated in the form of a Rate Contract by a nodal agency and economies of scale can be obtained
- **Single sourcing I Nomination:** In cases where the required Solution / Product is available from only one vendor and there are no suitable alternatives (strong justification required)

Two stage processes are most appropriate for systems with one or more of the below factors:

- Complex Business Applications, in which requirements are not clear yet
- Systems in which finalization of requirements will need industry inputs
- Extensive Software development
- Complex technologies (e.g. large scale data processing equipment)

In stage one of the two stage process, client's high level understanding of the business requirement presented in the EoI document. The EoI solicits response from bidders indicating their interest, and also suggestions from the bidder to refine the requirements. Valid suggestions from this stage are used for refining the requirements in the second stage (RFP stage).

Single stage processes are used in cases where Standard Technical products / service specifications (e.g. packaged software like Accounting, HRMS etc) are procured. In such cases, requirements can be specified to great degree of accuracy and bidders have no major design discretion. Also, market offerings are standardized and are comparable.

13.5 Request for Proposals

A Request for Proposal (RFP) is an invitation for suppliers, often through a bidding process, to submit a proposal on a specific commodity or service. The RFP process brings structure to the procurement decision and allows the risks and benefits to be identified clearly upfront.

The RFP will have to specify in great detail, the following requirements of the Buyer:

- Technical and Functional Requirements
- Bid Process and Commercial Specifications
- Contractual and Legal Specifications (including Master Services Agreement)

The RFP is usually structured in 3 Volumes with one Volume for each one of the above requirements.

Illustrative contents of Volume I of the RFP are the following:

- Introduction & Detailed Background of the Project
- Project Vision, Mission and Objectives
- Services Definition
- Detailed Scope of Work for the Vendor
- Functional Architecture & Requirements
- Technical Architecture & Requirements (including Security Requirements)
- People Architecture
- Other Requirements (e.g. Data Migration, Digitization etc)
- Timelines for implementation of the Project
- Project Deliverables

Volume II of the RFP presents the Bid Process and Commercial specifications. The contents of Volume II include (illustrative):

- Bidding Terms and Conditions (Guidelines for preparing proposal)
- Pre-qualification Criteria
- Technical Evaluation Criteria
- Bid Opening and Evaluation Process
- Evaluation of Commercial Bids
- Negotiations, Contract Finalization and Award
- Formats for providing bid response
    - Pre-qualification
    - Technical
    - Commercial

This Volume provides the criteria for evaluating the bidders. In a 3 stage evaluation, the pre-qualification stage is used to ensure bids from those bidders who have the necessary technical and financial capabilities are evaluated. For this, the number of years the company is in operation, financial capability (turnover, profit etc), and past credentials are evaluated.

The Technical Bid is evaluated against pre-defined criteria. The following criteria are used to evaluate technical bids (illustrative):

- Technical Solution proposed by the vendor
  - Proposed solution and its compliance to functional requirements
  - IT Infrastructure and Hardware Design
  - Security Architecture
- Approach & Methodology
  - Project Management, Risk Management & Quality Management approach
- Past Credentials
  - Specific experience of projects similar to the current project
  - Broad experience in related domains
- Proposed Personnel
  - Quality of staff proposed for key roles
  - Quality of manpower available with the company

The final selection of the successful bidder may be through a number of selection methods.
Based on the department's requirements, any of the following methods may be chosen:

- Quality and Cost Based Selection (QCBS)
- Quality Based Selection (QBS)
- least-Cost Selection (l1)
- Fixed Budget Selection (FBS)
- Consultants' Qualifications Selection

QCBS takes into account both the quality of the technical proposal and the cost of the services to be provided. It provides a reasonable tradeoff between quality and cost, with Technical proposals are given weight of 60-90%, with minimum cut-off at 60-75%. The Technical proposals are marked in a scale of 0-100, while the commercial bids score are normalized to 100 with the lowest bidder scoring 100, other bidders will be scored proportionately.

Quality-based selection (QBS) is a method based on evaluating only the quality of the technical proposals and the subsequent negotiation of the financial proposal and the contract with the consultant who submitted the highest ranked technical proposal. QBS is appropriate when:

- Assignments are complex or highly specialized making it difficult to define precise Terms of Reference and the requires input from the consultants
- Assignments where the downstream impact is so large that the quality of the services is of overriding importance for the outcome of the project
- Assignments that can be carried out in substantially different ways such that financial proposals maybe difficult to compare

Least Cost Selection (LCS) is only appropriate for selecting consultants for very small assignments where well-established practices and standards exist. In LCS, a minimum quality mark is set for Technical score and selection of the lowest financial proposal from the companies that are above the cutoff. The process followed in LCS is given below:

- Technical proposals will be opened first and evaluated.
- Bidders securing less than the minimum qualifying mark will be rejected, and the financial

proposals of the rest will be opened and compared

- The firm with the lowest price shall then be selected and invited to negotiate and finalize the contract.

13.6 Some Considerations for Commercial Bid Formats

The formats for commercial bids should be such that, all bidders should be on a level playing field - with knowledge of all cost components in the project.

In case of bought out mode of operation:

- Overall commercial quote to be obtained under logical heads (Software development cost, Deployment hardware cost, AMC cost etc)
- Component level cost to be obtained under each major head

In case of PPP/ transaction fee based model:

- Bidder to be provided with all possible cost components and their quantity required over the contract period
- Bidder to be provided historical data and trends to project the expected transactions during contract period
- Individual cost components to be sought, in case of items under re-imbursement (e.g. hardware, consumables etc)

14. Contract Management Aspects

14.1 Importance of Contracts in e-Governance Projects

The reason for failure of many e-Governance projects can be traced back to lacunae in Contract development, which leads to:

- Losing control over the supplier/ vendor who is managing the project
- Appropriate skills and resources to the management of their contracts are not allocated
- Despite the critical nature of the contracts, it do not address contingency plans and risk management with clarity
- Service levels for the supplier / vendor are not addressed properly
- Inadequate key performance indicators to measure and drive the performance of supplier
- Business never remains constant and so does a contract. Reviews on the contract are not done regularly

A Contract may be defined as ""An agreement concerning promises made between two or more parties with the intention of creating certain legal rights and obligations upon the parties to that agreement which shall be enforceable in a court of law." Contract Management is the final stage of Procurement cycle. The Contract includes all administrative activities associated with administering a contract after it is executed, including a review of the completed contract.

The level of contract may vary from simple to complex contract. The degree of effort put into contract management should commensurate with the value, risk and complexity of the contract. In many e-Governance projects, the contract documents are prepared post award of contract to a vendor leading to:

- Lack of clarity on specific terms and conditions of the contract during bidding processes - bids prepared based on assumptions
- Dispute / disagreement on terms and conditions of the contract between selected vendor and government (as these terms are known to vendor / government post award of contract)
- Significant time consumed in finalizing / agreeing on the terms - delaying the project and in some cases award of contract to a new vendor.

To avoid such issues, the best practice is to prepare a Draft Master Service Agreement and provide it to bidders as part of the bidding document (Volume III).

14.2 Key Components of e-Governance Contracts

Based on the type of project, there can be templates prepared for Contracts, which addresses most of the Contract considerations. In general, the Contract contents can be divided into the following (illustrative):

- Project Specific Information: Contract contents specific to the project
- General Conditions of the Contract: Contract clauses which are more or less common across all projects of the same type
- Special Conditions of the Contract: Any specific changes introduced to the General Conditions, based on specific project requirements
- Appendices

The project specific information will have to be drafted for each project. The components that make up the project specific information include (illustrative):

- Scope of services / work for the vendor
- Deliverables
- Project Locations
- Project timelines/project schedule
- Project Duration
- Acceptance criteria for the deliverables
- Payment schedule
- Obligations / Responsibilities of the Department
- Service Levels / Performance Indicators and Service Level Agreement
- Penalties /Incentive measures (if any)
- Scope change management approach etc

The contract will inter-alia include the RFP (all Volumes) and all its Annexures and the Technical and Commercial proposals of the bidder,

The General Conditions / Common Terms of Contracts include:

- Definitions of Terms used in the Contract
- Conditions precedent to contract signing
- Applicable Law governing the Contract
- Currency of the contract
- Language of the contract and administration
- Authorized representatives of the department and vendor
- Conditions on Taxes and Duties applicable for the contract, change in tax and duties and impact to project cost
- Approach for modifications or variations to the contract
- Breach, Rectification and Termination
- Protections and Limitations
- Intellectual Property Rights
- Force majeure
- Conditions for suspension and/or termination of contract
- Liabilities of parties
- Dispute resolution approach
- Exit management
- Arbitration and courts for dispute resolution

These terms remain more or less constant in the same project category, and hence can be provided in a template form. This allows for elimination of human errors, and adoption of best practices in Contracts.

14.3 Common Terms of Contract

Some of the common clauses in contracts are discussed in this section.

Breach, Rectification and Termination clauses

This clause specifies the terms relating to termination of the Agreement by either party, in the event of material breach of obligations by the other party. The components of these clauses include:

- Process of termination:
  - Notice provided to the other party, detailing the material breach
  - Within the period given for response to the notice, the breach should be set right, failing which termination proceedings will start
- Reasons for Termination:
  - Material breaches (default in providing services as per the Agreement, delay of a period unacceptable to the client etc)
  - Change of control in SP (merger, amalgamation etc)
  - Apprehension of Bankruptcy of the Service Provider

Upon termination of contract, all related Agreements including SLAs will terminate and Exit Management clauses as defined in the Agreement will start

Protections and Limitations

The Protections and Limitations section provides the protection available to the Department and Service Provider, in various scenarios and provides the limitations of liability.

The clauses which are included in the Protections and Limitations section include:

- Warranties: assurance or guarantee by a seller promising to indemnify the buyer if the warranted fact proves to be untrue. Warranties may be express, implied or disclaiming warranty. In case of components manufactured by third party, the SP confirms the authority to enforce the warranties on behalf of the client to the third party
- Third Party Claims: protects the department against damages to third parties arising out of reasons attributable to Service Provider
- Limitation of Liability: is a concept whereby a Service Provider's financial liability in case of losses or damages is limited to a fixed sum, most commonly the aggregate amount received by the SP for delivery of services under the contract
- Force Majeure: clause in contracts essentially frees both contracting parties from liability or obligation when an extraordinary event or circumstance (force majeure) occurs. Force majeure events include acts of God like flood, drought, lightning, fire etc or act of government or other competent authority like war, terrorist attacks, riots etc
- Data Protection: Clauses to ensure that the in the course of compiling, processing and storing proprietary project data, the SP adheres to the applicable Data Protection Laws and requirements of the project
- Audit, Access and Reporting: clause mandates the SP to provide access to all information which is in the possession or control of the SP, which relates to the provision of the Services as set out in the Audit, Access and Reporting Schedule and is reasonably required to comply with the terms of the Audit, Access and Reporting Schedule.

Insurance and Taxes

The Contract should address the following insurance related issues:

- The type and amount of insurance coverage to be maintained by each of the parties, and party responsible for the cost of the coverage
- Commercial general liability insurance
- Insurance on software (OEM), Hardware
- Insurance for man power deployed

- Protection against any claims, suits, actions, costs, damages or expenses arising from the negligence or intentional acts or omissions of the other party

The Tax related clauses should address:

- Payments as specified in payment terms will be inclusive of all statutory levies, duties, taxes and other charges whenever levied / applicable
- The SP shall bear all taxes arising out of payments received under the contract

Contract Payments

The clauses governing payments made to the Service Provider are included in the Payment Terms Schedule. The Schedule should address:

- Total payment made under the contract and mode of payment (lump sum for project components based on milestone / man month rates / monthly transaction charges / unit prices etc)
- Prices quoted by the bidder in strong and stable currency and break down of the quoted prices
- Payment milestones and schedule
- Cost components to be covered by the SP in return of Contract Payment and Cost components covered by Department (e.g. Third Party Audit)
- Lead times for price changes
- How incidental costs arising in the project will be handled (e.g. Change Controls)

Dispute Resolution Mechanisms

Disputes arise due to the disagreements between the department and the vendor, in cases where no material breach has occurred (e.g. Quality of deliverables, any claim arising out of the Agreement etc). Disputes are addressed in accordance to the provisions of the Disputes and Amendments clause in the Contract.

The first level of dispute resolution is the Dispute Resolution Board (usually the Project Management Committee), consisting of representatives from the department and the Vendor. The decision of the PMC on the dispute shall be given within a specific number of days, as mentioned in the Contract.

14.4 Project Type Specific Aspects of Contracts

Different types of projects have different priority areas. The Contract clauses for a government owned bought out software development project may not be relevant in a PPP based service delivery project. The Contract clauses need to tailored based on specific project requirements, based on the type of project.

The Contract considerations for the following project types are explored in the subsequent sections:

- Software Development project
- IT Infrastructure projects
- Service Delivery projects
- Public Private Partnership

Many e-Governance projects may have a combination of more than one of the above types and contract clauses shall be suitably tailored.

14.5 Contract Aspects of Software Development Projects

The major considerations for a Software Development project are listed below:

Source Code Ownership and Intellectual Property Rights:

"Source Code" is the term for individual modules, class layers, images, and pieces of computer programming that are compiled together to make up your software system. Ownership of Source Code is an ethical and legal issue. "Bespoke Software" means the software designed, developed, tested and deployed by the SP for the purposes of rendering the Services as part of the project, including customization components to other third party software.

As per the Indian Copyright Act, 1957, the Copyright of the Software developed by a third party rests with the third party, unless obtained through a written deed of assignment. Accordingly, Software Development project should have a clause, assigning exclusive Intellectual Property Rights to the department:

- IPR to all the Bespoke Software developed , forms and the compilations of the project
- IPR to any logo, trademark, trade name, service mark or similar designations
- Exclusive rights to all project proprietary data
- For third party products for which the SP had IPR before the contract, IPR will continue to vest with the SP. But the department will have exclusive IPR to the project specific customizations on the product (e.g. Bolt-on built on top of an ERP product, developed specifically for the department)

Change Control Management:

In any Software development project, it is inevitable that changes will be required, from the original specifications. For a project of any complexity, the software will rarely be implemented as originally specified. "Change Control" is the mechanism for parties to agree scope and cost implications of a particular change (whether amendment to the MSA / Service Level Agreements or service change).

Some of the reasons which result in Change Control being necessitated:

- Changes in processes / addition of a new process
- Scope expanded to include additional functionalities
- New services introduced by department

The change control procedure should be detailed in the contract and should set out the steps of suggesting, documenting, pricing and implementing variations. The prices for change control should be derived from the unit prices in bid, as much as possible.

Exit Management:

This clause sets out the provisions which will apply on expiry or termination of the "Contract Agreement", the "Project Implementation, Operation and Management SLA (Service Level Agreement)" and "SOW (Scope of Work)". Exit Management ensures smooth transition at contract expiry, to a new Operations & Management vendor (or in some cases, internal IT team of department).

The Exit Management Schedule details the following:

- Cooperation and provision of information by the SP
- Handing over confidential information and data of the project to the department
- Transfer of project assets
- Transfer of Certain Agreements
- Transfer Costs on transfer of project assets to the department
- General Obligations of the SP
- Exit Management Plan

If exit management is not properly planned, high termination costs might arise. These costs may be due to:

- Intellectual Property Rights not transferred to the department
- Assistance from incumbent vendor to transition to third party not provisioned in the Contract
- No provisions in the Contract to calculate residual value of equipment and other assets
- Transfer of Assets or any remaining payables (e.g. lease payments)

All these can be eliminated by having a well designed exit management clause in the Contract. Specific clauses should also be put in place in the contract to ensure knowledge transfer to the new vendor on exit.

Acceptance Testing, Audit & Certification of Projects

The primary goal of Acceptance Testing, Audit & Certification is to ensure that the proposed system meets requirements, standards, and specifications as required by the client and as needed to achieve the desired outcomes. The contract clause should clearly specify the scope of acceptance testing, the testing schedule, evaluation criteria and the threshold limit for service levels.

A Third party audit may be carried out to ensure compliance to the requirements set out by the department:

- Concurrent audit - Audit carried out in parallel with design, development and implementation to certify deliverables at each stage
- Certification audit - Audit carried out once the Software is fully developed and ready for deployment

The scope of audit usually involves Functional Requirements compliance, Interoperability and adherence to standards, Meeting of Service Levels, Controls review and Security Audit.

Other considerations for Software development contracts:

- **Documentation:** Contract to ensure that project documentation is updated by SP at specified intervals and latest documentation to be maintained with the department
- **AMC for system software:** In case of third party system software (Database Servers, Operating Systems), the SP should have AMC arrangements with the OEM for the contract period.
- **Licensing Policies and Upgrades:** The Licenses to the System Software and other licensed products should be obtained in the name of the department. Any upgrades updating of patches / service packs / fixes from product vendors should be provisioned to be provided free of cost by the SP
- **Post Implementation Support:** The contract should have special mention of the clause for duration of support from the service provider/ OEM for the implemented IT solution. This should include time duration for which the support will be required, type of support required and support required for complete solution/ particular modules.

14.6 Contract Aspects of IT Infrastructure Projects

Warranty Terms for IT Infrastructure

Warranty ensures sustainability and assurance or guarantee by a service provider/ OEM to the client. The Warranty clause should detail the following:

- Warranty period (subject to the warranty period provided by the OEM)
- Date of commencement and commissioning
- Type of warranty (Express / Implied / Disclaiming)
- Warranty coverage

- Cost arrangements

The contract clause should clearly specify the kind of arrangements that the service provider should have with the product supplier / manufacturer (Tripartite / Back to back arrangement).

Audit & Certification of IT Infrastructure

The purpose of the audit is to ensure IT infrastructure deployed is as per the specifications provided in the Request for Proposal. The other aspects of audit include:

- To audit Quality as per ISO 9126
- Reliability
- Availability
- Efficiency/ Performance
- Usability
- To audit Security compliance as per BS 7799 / ISO 17799

Exit Management Clauses

Exit Management is applicable when the O&M contract ends and the IT Infrastructure is handed over to the department. The Exit Management clauses should take into account the following considerations:

- Transfer of Assets
    - Project assets including Hardware, Software, Documentation and any other infrastructure to be renewed and cured of any defects and handed over to the department
    - Basis of calculation of depreciated value of project assets (IT Infrastructure) to be specified in the Exit Management clause
    - Applicable transfer cost and stamp duty on transfer of project assets to be borne by the SP (except in case of termination due to department's default)
- Inventory / Stock management and transfer
- Condition of assets
- Transfer of project related agreements
    - Shifting of assignments, transfers, licenses and sub-licenses related to any equipment lease, maintenance or service provision agreement between SP and any third party to department / new SP appointed by the department
- Documentation relating to IT infrastructure supply and installation
- Terms of payment / penalties, during exit
- Legal terms for exit
- Calculation of true value of assets (basis of calculation of depreciation)

Other Considerations for IT Infrastructure Contracts

Other considerations specific to IT Infrastructure projects include:

- **Scope of Consumables:** Contract to specify the scope of supply and usage of consumables.
- **End of Life:** Clauses to ensure that the IT Infrastructure components are not in the end of their product Lifecycle and support is assured during contract period
- **Documentation:** Ensuring that up to date documentation is available with the department

- **Insurance:** Cost of insurance for components to be borne by SP
- **Spares and Replacements SLA:** SLA clauses to address quick delivery of spares and fixing of defects in the IT Infrastructure
- **Hours of Support:** Working hours for the support staff for IT Infrastructure maintenance

14.7 Contract Aspects of PPP and Service Delivery Projects

The following aspects should be covered in PPP and Service Delivery projects:

- Transfer of Assets: Contract to provide clarity on ownership and transfer of assets created for the project (service delivery centers, related infrastructure etc)
- Usage of government facilities for non government transactions: Contract should specify the following terms:
    - Contract to clarify whether any non-government services can be delivered through the service delivery channels (for increasing project viability e.g. payment of mobile bills for private operators through CSCs)
    - If yes, approach for addition/deletion of such services
    - Revenue sharing (if needed)
    - Avoiding conflict of priority between government and private services
- Funds management:
    - Remittance and accounting procedures for collection of payments and taxes
    - Payment of transaction fees (deduction at source by vendor or payment based on quality of services?
- Hours of operations: Working hours for service centers or call centres, support needed for online service delivery channels.
- Liability and responsibility of Service Provider in case of fraudulent transactions:
    - Liability to be with the SP in cases of claims / damages against the department in case of fraudulent transactions
    - SP to arrange for insurance coverage, at its expense, for cases of third party claims
- Revenue Sharing Model:
    - How will revenues from the project be shared between the Government and the Service Provider?
    - What are the safeguards in place to prevent excess payout from government, in case transactions are much higher than projected numbers (transaction fee based model with cap, sliding scale etc)
    - What safeguards are the vendor provided in cases of projected transactions not materializing (upfront payment for certain components e.g. IT Infrastructure)
- Addition / Deletion of new Services I Service Delivery Channel:
    - In case of addition / deletion of new Services / Service Delivery Channels, the modality of revenue sharing, renegotiation of transaction fee for other services etc should be addressed
    - Interests of department and the SP to be taken into account in designing the modalities (deletion may result in lower payout to SP, addition may result in higher payout)

14.8 SLA and Service Level Management

Service Level Agreements are an integral part of any e-Governance Contract. In any e- Governance Project, Government is essentially buying services, and not hardware, software & networks. Service Level Agreement (SLA) framework defines the minimum levels of service to be maintained by the Service Provider.

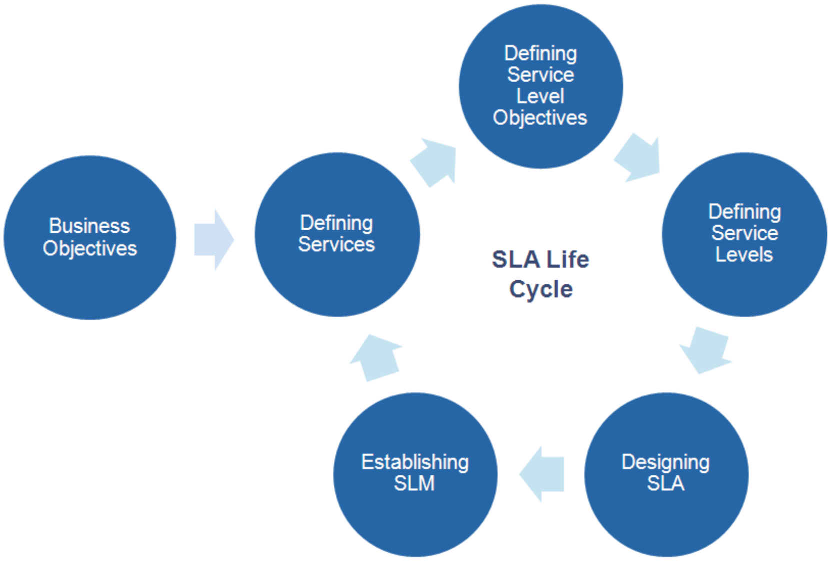
Some of the definitions related to Service Level Management are given below:

- Service: A Service is an outcome of a request and it provides an economic, social or personal benefit or right to the requestor or results in efficiency gains to an organization.
- Service Level: A Service Level defines the quality and quantity of service, in a measurable and objective way.
- Service Level Objective (SLO): is the set of purposes or objectives sought to be achieved through defining and prescribing the Service Levels for an initiative or organization.
- Service Level Agreement (SLA): is an agreement between the Service Provider and the Service Seeker that defines the Service Levels, the terms and conditions for enforcing the Service Levels and the remedies in case the Service Levels are not fulfilled.
- Service Level Management (SLM): is an institutional arrangement that ensures effective implementation of the Service Levels and enforcement of the SLA

In government scenario, there are a lot of challenges in managing and monitoring SLA terms. Accordingly, certain design criteria should be kept in mind while designing SLAs. SLAs should be:

- Be simple to apply in a field situation
- Cover ALL the services envisaged in the Project.
- Lay emphasis on different services in proportion to their relative values to the stakeholders.
- Be measurable through automated tools.
- Be Precise and Unambiguous.
- Be equitable as between the Service Provider and the Service Seeker.
- Be cost-effective to implement.
- Be legally enforceable.
- Provide scope for evolution of SLA into a more mature state

The SLA Lifecycle is shown below:



Business Objectives are defined based on - Vision and Mission of the Organization, Business Drivers and Desired Business Outcomes. Services are listed down based on the business objectives. For each service, Service Level Objectives are defined. SLO is the value that the management intends to give to various sets of stakeholders, and the value it intends to derive from the investment in Technology and Infrastructure. Illustrative SLO are given below:

Stakeholder Group	Value Proposition (SLO)
External: Customers, Suppliers, Financiers	Efficiency, Convenience, Reliability, Responsiveness, Cost Effectiveness
Internal: Employees, Management, Auditors	Usability, Accountability, Traceability, Effectiveness

Investment Area	Value to be derived (SLO)
Technology & Process: Standards, Architecture, BPR	Interoperability, Cost Effectiveness, Transformation, Simplicity
Infrastructure & People areas: Data Centre, DR Site, Change Management	Performance, Security, Availability, Efficiency, Ownership

The next step is the definition of Services Levels for each service delivered by the department. Service Levels defined for those services to be delivered by the Vendor forms the basis of the Service Level Agreements. The components of the Service Level Definition are:

- Service Level Parameters: measurable attributes of the service, which will provide a reliable and objective estimate of the quality and quantity of service
- Service Level Metrics: A set of norms prescribed against each service level parameters to provide baseline performance expected from Vendor
- Service Level Measurement Method: Precise, reliable and consistent method by which the service level parameter can be measured
- Service Level Enforcement Method: Method by which the service level agreement can be enforced (deduction from payments, penalties etc)

The Service Level Parameters should fulfill the following criteria:

- Alignment with Service Level Objectives
- Coverage of complete range of services under the project
- Number of SLPs in each service area and their weightage should correspond to the priority of the service area
- The number of SLPs should not be excessively large, affecting the ease of SLA monitoring
- If required, SLPs may be defined for different phases of the project, based on the priorities of each phase (e.g. System Development phase, Pilot phase, Operations and Maintenance phase)

Service Level Metrics (range of values) are the performance metrics defined for each service level parameter:

- Baseline: Acceptable level of service by the vendor
- Lower: Degraded level of service, for which vendor may be penalized
- Higher (optional): Higher level of service for which vendor may be incentivized

- Breach: Highly degraded level of service / material breach, which may invite termination contract

Service level metrics should be realistic without compromising on Service Level Objectives.

SLA can be most effectively enforced by linking the payments to the Service Provider to the degree of compliance with the SLA. The various methods of achieving this include:

- Deduction Method:
    - Vendor gets 100% payments (monthly / quarterly / milestone) for full compliance to the SLA
    - For lower performance from SLA, specified percentage is deducted. Higher performance may be incentivized by bonus payments
- Addition Method:
    - A percentage of the payment (e.g. 40%) to the SP is made dependant on the fulfillment of Service Level Matrix
    - All SLPs are assigned credits for baseline, lower, higher and breach metric.
    - Credits will depend on the priority of the SLP
    - Scores prescribed for baseline performance will add up to 100%

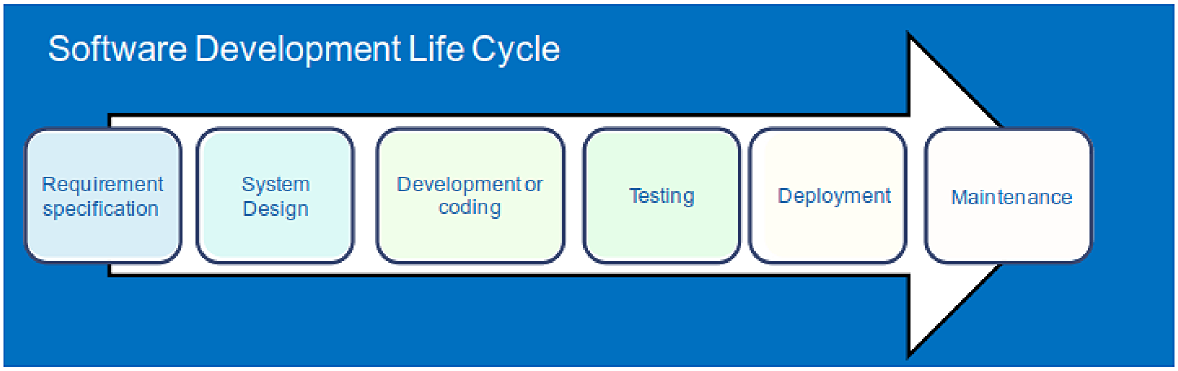
Automated SLA metric measurement and automated SLA calculation based on performance should form part of the Functional Requirements, in case of Software development projects.

15. Software Development Lifecycle

This section provides an overview of software development Lifecycle, its key phases, activities and outputs at each phase of the Lifecycle. This section also presents a brief overview of various software development models followed in general.

15.1 Overview of Software Development Lifecycle and Models

The Software Lifecycle models the evolution of a product from opportunity identification to its end-of-life. It is designed to build on one another, taking the outputs from the previous stage, adding additional effort, and producing results that leverage the previous effort and are directly traceable to the previous stages. This top-down approach is intended to result in a quality product that satisfies the original intentions of the customer. It is a structured approach for creation of IT systems/software systems and provides guidance on phases of systems development, activities and outputs at each phase and addresses Quality Assurance requirements at each phase of the Lifecycle and for each deliverable. It also covers standardization of processes for systems development across organizations to improve software quality, maintainability. Following provides typical route Lifecycle for software development and implementation.



There are several software development models existing, but in general there are three Lifecycle approaches. These are:

Development Approach	Development Models
Sequential	• Build and fix model • Waterfall model • Iterative waterfall model
Iterative	• Iterative model • Spiral model • Incremental model • Evolutionary model • Component based development • Rapid application development model • Rational unified process
Recursive	• Fountain model • Recursive multi thread model

Table below presents a brief overview of some key software development models.

SDLC Model	Key Features
The waterfall model	• Also known as the linear sequential model, with its major phases, milestones, and products. • Can be successfully used when requirements are well understood in the beginning and are not expected to change or evolve over the life of the project • The output from one phase serves as the input to the next phase, with the project flowing from one step to the next in a waterfall fashion • Highly structured development process and is the "traditional" approach to software development • Considered superior to the previously used "code and fix" methods of software development, which lacked formal analysis and design
Incremental Model	• The incremental model is essentially a series of waterfall cycles • The incremental model prioritizes requirements of the system and then implements them in groups • Each subsequent release of the system adds function to the previous release, until all designed functionality has been implemented • Each development cycle acts as the maintenance phase for the previous software release • this model assumes that most requirements are known up front
Structured Evolutionary Prototyping Model	• The evolutionary model, like the incremental model, develops a product in multiple cycles. • Unlike the incremental model, which simply adds more functionality with each cycle, this model produces a more refined prototype system with each iteration. • Developers build a prototype during the requirements phase • Prototype is evaluated by end users • Users give corrective feedback • Developers further refine the prototype • When the user is satisfied, the prototype code is brought up to the standards needed for a final product
Rapid Application Development Model (RAD)	• Rapid Application Development uses minimal planning in favor of rapid prototyping. • The "planning" of software developed using RAD is interleaved with writing the software itself • The structured techniques and prototyping are especially used to define users' requirements and to design the final system. • RAD approaches may entail compromises in functionality and performance in exchange for enabling faster development and facilitating application maintenance.

The following table provides for comparison of these software development models.

Requirement	Waterfall	Incremental	Evolutionary
Requirements are known and stable.	ü	ü	
User needs are unclear/not well defined			ü

An early initial operational capability is needed.		ü	ü
Early functionality is needed to refine requirements for subsequent deliveries.		ü	ü
Significant risks need to be addressed.		ü	ü
Must interface with other systems	ü	ü	
Need to integrate new technology.			ü
Software is large or complex	ü	ü	ü
Software is small or limited in functionality		ü	ü
Software is highly interactive with user		ü	ü
Software involves client/server function	ü	ü	ü
Follow initial cost and schedule estimates	ü	ü	
Detailed documentation necessary	ü	ü	
Minimize impact on current operations	ü		
Full system must be implemented	ü	ü	
Reduce the number of people required		ü	ü
Project management must be simpler	ü	ü	
System must be responsive to user needs		ü	ü
Progress must be demonstrated early		ü	ü
User feedback is needed		ü	ü
Reduce the costs of fixes and corrections		ü	ü

Following discusses the key activities performed at each phase of software development including key inputs and outputs.

Stage 1: Requirement Definition

Overview of Stage	Key Activities Performed in the Stage
• Definition of the need to acquire a system, software product or software service • Definition of goals for the proposed software development • Refine each goal into a set of one or more requirements • These requirements define the major functions of the intended application, define operational data areas and reference data areas, and define the initial data entities.	• Planning and Initiation; • Identification of objectives • System study • Requirement analysis

Inputs	Outputs
• Vision and objective • High-Level Requirements	• Requirements Document • Requirements Traceability Matrix • Project Plan & Schedule

Stage 2: System Design

Overview of Stage	Key Activities Performed in the Stage
• This phase is the first step in moving from problem domain to the solution domain • The design stage takes as its initial input the requirements identified in the approved requirements document. • For each requirement, a set of one or more design elements will be produced as a result of interviews, workshops, and/ or prototype efforts. • Design elements describe the desired software features in detail, and include: • Functional hierarchy diagrams • Screen layout diagrams, • Business process diagrams, • Pseudo code, • Complete entity-relationship diagram with a full data dictionary.	• System analysis • System Functional Review • Development of Software Design Document
• Design elements are intended to describe the software in sufficient detail that skilled programmers may develop the software with minimal additional input. • When the design document is finalized and accepted, the Requirements Traceability Matrix is updated to show that each design element is formally associated with a specific requirement.	
Inputs	**Outputs**
• Requirements Document	• Design Document • Updated Requirements Traceability Matrix • Updated Project Plan & Schedule

Stage 3: Development or coding

Overview of Stage	Key Activities Performed in the Stage

• The goal of the development phase is to translate the design of the system into code in a given programming language • Takes design elements described in the approved design document as input and for each design element, a set of one or more software artifacts will be produced. • Software artifacts include but are not limited to menus, dialogs, data management forms, data reporting formats, and specialized procedures and functions • The outputs of the development stage include a fully functional set of software that satisfies the requirements and design elements previously documented • Appropriate test cases will be developed for each set of functionally related software artifacts • A test plan is developed that describes the test cases to be used to validate the correctness and completeness of the software • The RTM will be updated to show that each developed artifact is linked to specific design element, and that each developed artifact has one or more corresponding test case items.	• Development of System Architectural Design • System Requirements Analysis • Process Implementation

Inputs	Outputs
• Design Document	• Software • Implementation Map • Test Plan • Updated Requirements Traceability Matrix • Updated Project Plan & Schedule

Stage 4: Testing

Overview of Stage	Key Activities Performed in the Stage

• Testing is the major quality control measure employed during software development. Its basic function is to detect errors in the software. • During requirement analysis and design, the output is a document that is usually textual and non-executable. After the implementation phase, computer programs are available that can be executed for testing phases. • Testing not only uncovers errors made during coding, but also errors introduced during the previous phases. Thus, the goal of testing is to uncover requirement, design or coding errors in the programs. • During the test stage, the software artifacts, and test cases are migrated from the development environment to a separate test environment • Successful execution of the test suite confirms a robust and complete migration capability. • During this stage, reference data is finalized for production use and production. The final reference data (or links to reference data source files) and production user list are compiled into the Production Initiation Plan. • The outputs of the integration and test stage include an integrated set of software, an online help system, an implementation map, a production initiation plan	• Software Qualification Testing • System Acceptance Testing • Software Acceptance Support **Types of Testing** • Black box testing • White box testing • Unit testing • Integration testing • Functional testing • System testing • Regression testing • Acceptance testing • Load and Stress testing • Performance testing

Inputs	Outputs
• Software • Implementation map • Test plan	• Test results • Gaps in the system

Stage 5: Testing

Overview of Stage	Key Activities Performed in the Stage

• The software artifacts and initial production data are loaded onto the production server. • All test cases are run to verify the correctness and completeness of the software. • Upon satisfactory verification of production data and the test suite has been executed with satisfactory results, the customer formally accepts the delivery of the software	• Process implementation; • Operational testing; • System operation; • User support.
Inputs	**Outputs**
• Production initiation plan • Acceptance plan • Integrated plan • Implementation map	• Production Software • Completed acceptance test • Customer acceptance memorandum • Archived software artifacts • Archived project plan and schedule

Stage 6: Maintenance

Overview of Stage	Key Activities Performed in the Stage
• Maintenance includes all the activity after the installation of software that is performed to keep the system operational • The maintenance phase involves making changes to hardware, software, and documentation to support its operational effectiveness. • It includes making changes to improve a system's performance, correct problems, enhance security, or address user requirements. • To ensure modifications do not disrupt operations or degrade a system's performance or security, organizations should establish appropriate change management standards and procedures.	• Problem and modification analysis • Modification implementation • Maintenance review /acceptance • Migration

Inputs	Outputs

• Production Software • Production initiation plan • Test plan • Implementation map	• Post-Implementation Review • Verify Operations Support materials updated

16. Project Management for e-Governance Projects

16.1 e-Governance Project Management

e-Governance is not simply a matter of giving government officials computers or automating old practices. Neither the use of computers nor the automation of complex procedures can bring about greater effectiveness in government or promote civic participation. Focusing solely on technological solutions will not change the mentality of bureaucrats who view the citizen as neither a customer of the government nor a participant in decision-making. Understood correctly, e-Governance utilizes technology to accomplish reform by fostering transparency, eliminating distance and other divides, and empowering people to participate in the political processes that affect their lives. Governments have different strategies to build e-Governance. Some have created comprehensive long-term plans. Others have opted to identify just a few key areas as the focus of early projects. In all cases, however, the countries identified as most successful have begun with smaller projects in phases on which to build a structure.

The success of an e-Governance project depends upon the development of the project in an integrated and holistic manner. e-Governance should not be understood merely as the procurement of hardware and other networking equipment. e-Governance is an integration of various fields of management thus making it a management game rather than merely a technology enabled project.

16.2 Need for Project Management

The e-Governance initiatives can be divided into three categories:

- Total failure: the initiative was never implemented or was implemented but immediately abandoned.
- Partial failure: major goals for the initiative were not attained and/or there were significant undesirable outcomes.
- Success: most stakeholder groups attained their major goals and did not experience significant undesirable outcomes.

The following statistics provides the success rate for the e-Government projects.

Trends on e-Government initiatives in developing / transitional countries
• 35% are total failures • 50% are partial failures • 15% are successes

Critical factors resulting in failure of e-Governance projects are:

- Unrealistic or unarticulated project goals
- Inaccurate estimates of resources
- Badly defined system requirements
- Poor reporting of the project's status
- Unmanaged risks
- Poor communication among customers, developers, and users

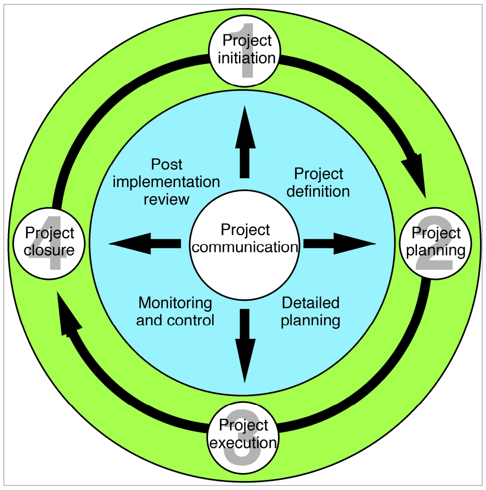
- Use of immature technology
- Inability to handle the project's complexity
- Sloppy development practices
- Poor project management
- Stakeholder politics
- Commercial pressures

These failures come at a high price for the world's poorer countries, and six categories of potential costs of e-Governance failure can be identified:

- **Direct Financial Costs.** The money invested in equipment, consultants, new facilities, training programs, etc.
- **Indirect Financial Costs.** The money invested in the time and effort of public servants involved.
- **Opportunity Costs.** The better ways in which that money could have been spent, if it was not spent on the e-Governance failure.
- **Political Costs.** The loss of 'face' and loss of image for individuals, organizations and nations involved in failure.
- **Beneficiary Costs.** The loss of benefits that a successful e-Governance project would have brought.
- **Future Costs.** An e-Governance failure increases the barriers for future e-Governance projects. It does this in two main ways. First, through loss of morale of stakeholders, particularly e-Governance champions, who may 'defect' to the private sector or overseas. Second, through the loss of credibility and loss of trust in e-Governance as an approach to change. This increases risk aversion in some stakeholders; and provides support for others with vested interests in the status quo.

Government has prioritized adoption of e-Governance as a key strategy to improve governance particularly in providing significantly improved services to citizens and businesses. To achieve these objectives, specific, measurable goals and time frames for each e-Governance project need to be clearly identified at the outset.

16.3 Project Management for e-Governance Projects



The Lifecycle of e-Governance projects is a continuous circular chain of activities, divided into four phases: Initiation, Planning and Implementing, Operations and Monitoring.

Initiation

This is the phase in which Governments first articulate their intention and vision which will ultimately lead to Service Transformation. If Service Transformation is the ultimate outcome of the Lifecycle Process, Initiation will be the very beginning. It is articulated in a vision statement - a statement of intent of the Government to embark on this journey. It is perhaps the most important phase, as all other subsequent phases will depend largely on the clarity and realism that is incorporated in the first phase. The boundaries of e-Governance systems, the services to be provided, the resources necessary for planning and implementation, operations and monitoring would be defined in this phase.

Planning and implementing

Typically, human and financial resources are two most important factors that contribute to success. Applications must be deployed to provide the services specified, but also at the right time, so that user take-up is optimized. Change management is another important issue in this phase. Typically, again, several applications can be developed simultaneously ranging from the simple to the extremely complex. Getting rid of silos and allowing sharing of information is one of the goals of e-Governance, and coordination to ensure inter-operability is another concern. This and issues of technology, user friendliness, availability, scalability, ownership and pricing of services will dominate this phase.

Operations

The operations phase has two objectives. The first is reliable day-to-day operations and the second is the progressive integration of systems to achieve service transformation.

Monitoring

Monitoring relates to optimization of services. e-Governance projects can take a long time to permeate. Confidence of users to transact business through the impersonal machines does not come easily. It needs strong day-to-day monitoring. Building up the services, capturing and resolving customer feedback are prime concerns during the monitoring phase.

Risks

Within each phase of the lifecycle we have addressed the issues that were identified as the main challenges and risks to e-Governance, during the work with the last report "Auditing e-Governance". By doing so, we also saw a need to identify different risks depending whether they were related to a state and government level or a department level. The issues and risks are therefore sorted accordingly within the four phases of the Life.

16.4 Project Management guidelines for e-Governance Projects

Government has prioritized adoption of e-Governance as a key strategy to improve governance particularly in providing significantly improved services to citizens and businesses. To achieve these objectives specific, measurable goals and time frames for each e-Governance project need to be clearly identified at the outset. Competent professional advice needs to be obtained, using consultants wherever necessary, to deal with the complex issues involved in the task as well as to decide on the most appropriate strategy for implementation. Finally, a transparent bid process needs to be adopted to identify and select the implementing agency. While these general principles are well understood, the process to be adopted for this purpose is not.

These guidelines help improve understanding the issues related to implementation of e-Governance projects. Implementation of e-Governance is a phased program involving the four stages: The guidelines for each phase of the project are explained as follows.

Stage I: Conceptualization

Conceptualization is the most crucial phase of an e-Governance project. The purpose of this phase is to attain clarity on the benefits and the outcomes of the proposed initiative. The deliverables of this phase include-

- A well-articulated vision statement, a sharp mission statement and a set of specific objectives of the proposed project / initiative.
- The list of customer-centric services.
- The outcomes or benefits to stakeholders like improvements in speed, convenience of access, transparency, efficiency of services etc.
- The mix of delivery channels appropriate to deliver the services in a convenient and affordable manner.
- An estimate of Transaction Cost

- A consultation with the stakeholders to derive / validate the list of services, outcomes, delivery strategy and the transaction costs.
- A high-level functional architecture showing the transformed business processes.
- A high-level technology architecture that can translate the functional architecture into a reality. A clear Business Model.
- A Project Proposal/ Document (Detailed Project Report or DPR) encompassing all the above components.

Contents of a Typical DPR would include:

- Introduction
- Clearly laid out objectives
- Target Beneficiaries
- Existing e-Government services
- Newly proposed services
- Business Process Reengineering - BPR
- Technology Option adopted
- Functional Requirement Specifications (FRS)
- Project Management structure
- Detailed AS-IS Scenario
- Detailed TO-BE Scenario
- Change Management methodology
- Capacity Building
    - Department e-Government group for change management / process change
    - For overall implementation of the e-Government Project
- Financials
    - Means of Project Finance
    - Cost estimates
    - Evaluation of Options
    - Phasing of Expenditure
    - Options of Cost Sharing and Cost Recovery
    - Models of PPP like BOO,BOT, BOOT to etc. to be considered
    - Leveraging of existing core IT infrastructure (SWAN, CSC, SDC)
- Phased Time Frames

The DPR should also contain sections on:

- Government Support
    - Legislative changes/legal amendments,
    - Infrastructure etc.
- Sustainability
    - Means of sustaining the project benefits
    - Means of replicating the project success
- Impact Assessment
    - Evaluation methodology of the Impact Assessment Study
    - TPA

It is desirable to establish an Empowered Committee, headed by the Secretary of the Nodal Department responsible for all major decisions connected with the project (like deciding on project objectives, outlays, implementation strategy, scope for attracting private investment, transaction costs, award of the project etc.), a Project Implementation Committee responsible for all operational decisions connected with the project (like changes of procedure, forms, etc., bidding parameters, specific service levels, etc.) and to nominate a Mission Leader/ Project Leader who would build a project team to drive the implementation and be responsible for achieving mission goals and timelines.

17. Monitoring and Evaluation

e-Governance project should be aimed at achieving business benefits to the Government and citizens. As discussed in the earlier sections, the first and foremost activity in undertaking an e-Governance project is to establish a clear vision, objectives and benefits expected to be delivered by the project to the target stakeholders. It is imperative for the organizations to monitor and track achievement of stated objectives and benefits throughout the Lifecycle of the project. Hence, definition of a Monitoring and Evaluation (M&E) framework for the project is a crucial element in e-Governance project design and implementation.

17.1 Overview of Outputs and Outcomes

To understand Monitoring and Evaluation, it is essential to gain an understanding of difference between outputs and outcomes. Following explains the same in simple terms.

Outputs of e-Governance project are the deliverables generated by the government, consultants, implementation partners and associated stakeholders at various phases of an e-Governance initiative. These outputs, for e.g., include e-Governance vision & strategy, reengineered business processes, IT system, IT infrastructure, training etc. These outputs should be clearly stated in the scope of the project and based on the responsibilities allocated to various stakeholders. Outcomes refer to the desired result of an initiative undertaken to meet a need or solve a particular problem. Outcomes, for e.g., may include areas such as reduction of passport delivery time to 3 days, improvement in literacy rate by 15%, to minimize leprosy from 15% to 5% etc.

The outcomes relate to the business objectives and benefits defined for the project and are final results supported by intermediate outcomes (benefits milestones). Outputs are defined to measure program performance and outcomes focus on business performance. Following table summarizes the difference between outputs and outcomes with few examples.

Goals	Examples of performance indicators
Outputs • Reengineered processes • New ICT systems • Increased service coverage	• Comparisons of old and new business processes • Technical reviews of IT infrastructure, applications, and performance • Variety of available services • IT support capacity • Service training
Outcomes • Increased efficiency • Increased transparency and accountability • Higher-quality public services • Better access to services	• Financial and time savings in government activities • Public perceptions, such as user satisfaction and score cards • Financial and time savings for citizens • Increased public service timeliness and responsiveness • Reduced errors • Financial saving per transaction

Following table further illustrates output management versus outcome management.

	Output Management	Outcome Management
Focus	Manage costs, inputs, schedule, resources, deliverables	Manage outcomes, benefits, business results, portfolio
Deliverables	Gantt Charts, schedules, work plan, costs, estimates, progress reports, milestones, issues, earned value, PERT charts, etc.	Outcomes maps, outcomes registers, value cases, value assessments, value graph, governance reports or structures
Measures of Success	On-time, on-budget, delivery of specified change enabler (e.g., system, process), risk management	Initiative delivers on promised results, maximized business value of portfolio
processes	Project initiation, project monitoring, project close out, etc.	Initiative definition, value definition, portfolio selection, results attainment
project I initiative	Is accountable to the business sponsor for project deliverables Is accountable to the Program Manager for project execution	Facilitates the value case, ensures that the initiatives benefits are achieved
Timeline	From project planning to implementation	From program planning through implementation to results attainment

17.2 Overview of Monitoring and Evaluation

Monitoring & Evaluation refers to tracking the outputs and outcomes, respectively, as defined for the project. Monitoring relates to tracking the project progress, outputs and deliverables as per the defined program/project plan whereas evaluation refers to assessment on achievement of business objectives and benefits defined for the project. The table below provides overview and difference between monitoring and evaluation.

Monitoring	Evaluation

• Regular observation and recording of activities taking place in a project or program • Process of routinely gathering information on all aspects of the project • Involves giving feedback about the progress of the project to the sponsor, implementers and beneficiaries of the project • Tracks inputs and outputs and compares them to plan • Identifies and addresses problems • Ensures effective use of resources • Ensures quality and learning to improve activities and services • Strengthens accountability	• Is a selective exercise that attempts to systematically and objectively assess progress towards and the achievement of an outcome • An assessment of a planned, ongoing, or completed program to determine its relevance, efficiency, effectiveness, impact and sustainability • The intent is to incorporate lessons learned into the decision-making process • Determines program effectiveness • Shows impact • Strengthens financial responses and accountability • Promotes a learning culture focused on service improvement • Promotes replication of successful interventions to make resource decisions • Decision-making on best alternatives • Support of public sector reform / innovation

Following table summarizes outputs, outcomes, monitoring and evaluation for a project.

Level	Description	Frequency
Inputs	Resources that are put into the project. Lead to the achievement of the outputs	Continuous
Outputs	Activities or services that the project is providing. Outputs lead to outcomes	Quarterly
Outcomes	Changes in behaviors or skills as a result of the implemented project. Outcomes are anticipated to lead to impacts	Short to medium term
Impacts	Measurable changes in project status, Impact results are effects of the intervention.	long term

17.3 Understanding Evaluation Types

There are two types of evaluation in general i.e. outcome evaluation and impact evaluation/assessment. Table below summarizes outcome and impact assessment followed by few examples.

Type	Purpose
Outcome	1. Examines specific program outcomes and accomplishments. 2. What changes were observed, what does it mean, and if changes are a result of the interventions?
Impact	1. Gauges the program's overall impact and effectiveness. 2. Aims to strengthen design and replication of effective programs and strategies

Some illustrative examples:

Literacy Improvement Program

Direction	Inputs	Outputs	Outcomes	Impact
• Policy • Objectives • Goals	• Funding • Experts • Infrastructure	• Schools • E-Learning • Facilities • Teachers	• Increase in enrolment into schools • Improved pass % of students	• Improved reach to education • Increased literacy levels

Polio eradication program

Direction	Inputs	Outputs	Outcomes	Impact
• Policy • Objectives • Goals	• Funding • Medicines • Resources	• Health camps • Health campaigns	• Reduction in Polio % to <1	• Healthy citizens and health nation

e-Governance Project in Business Registration

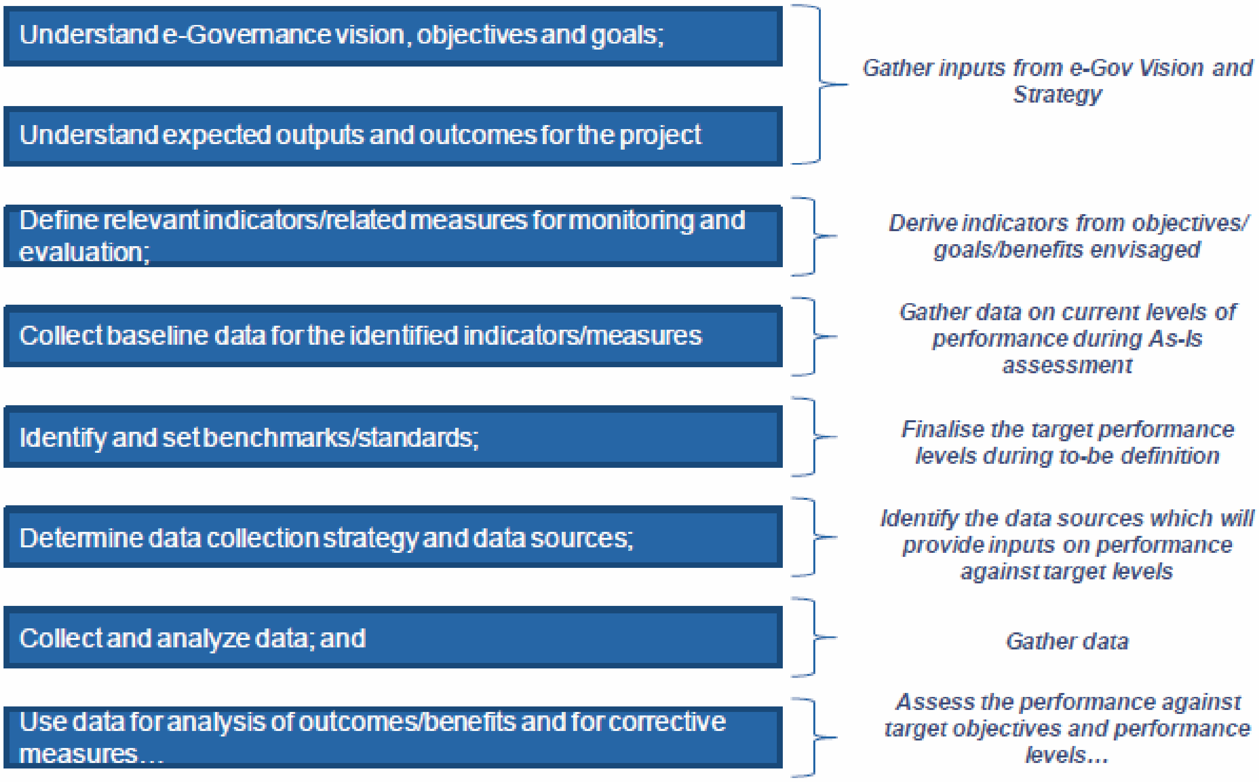
Direction	Inputs	Outputs	Outcomes	Impact
• Policy • Objectives • Goals	• Funding • Experts • Consultants • IT Specialists	• Reengineered processes • IT Systems • Computers for employees • Trained employees	• 80% of services provided online • 60% of transactions performed through self services • Reduction time for company registration from 60 days to 7 days	• Improved investment climate • Increased economic growth

e-Governance Project in Municipal corporations

Direction	Inputs	Outputs	Outcomes	Impact
• Policy • Objectives • Goals	• Funding • Experts • Consultants • IT Specialists	• Reengineered processes • IT Systems • Computers for employees • Trained employees	• Improved tax compliance monitoring • Increase in revenue by 30% • Increase in timely payment of tax by 15%	• Better civic infrastructure and amenities • Improved civic conditions in the corporation

17.4 Approach for development of M & E Framework

The diagram below provides an overview of approach for development of Monitoring and Evaluation framework for e-Governance projects.

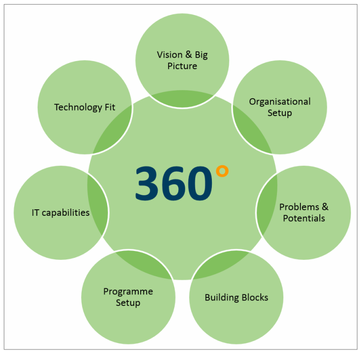

Understand e-Governance vision, objectives and goals;
Understand expected outputs and outcomes for the project
Gather inputs from e-Gov Vision and Strategy
Define relevant indicators/related measures for monitoring and evaluation;
Derive indicators from objectives/ goals/benefits envisaged
Collect baseline data for the identified indicators/measures
Gather data on current levels of performance during As-Is assessment
Identify and set benchmarks/standards;
Finalise the target performance levels during to-be definition
Determine data collection strategy and data sources;
Identify the data sources which will provide inputs on performance against target levels
Collect and analyze data; and
Gather data
Use data for analysis of outcomes/benefits and for corrective measures…
Assess the performance against target objectives and performance levels…

18. Framework for Assessment of e-Governance Projects

18.1 Overview of Outputs and Outcomes

18.1.1 Need for an assessment framework

The Department of Information Technology, Government of India, has felt it necessary to create a rational framework for assessing e-Governance projects on various dimensions. The justification for creation and use of such a framework is given below:



- **Significant investment of resources into e-Governance projects:** Significant national resources to the tune of about Rs.2,500 crores are going annually into implementation of e-Governance projects. Most of these projects are propelled by localized perceptions of the need to exploit ICT for better service, better efficiency and transparency. However, there is no evidence of any appraisal being done before the sanction / grounding of a project or during the period of its execution, as to whether the project is proceeding on the right lines to achieve its original objectives.
- **Subjective assessments & value judgment:** The rating of some of the e-Governance projects implemented in the country is currently based on subjective assessment and value judgment of a few individuals and authorizations. There is no authentic mechanism, much less an institutional mechanism, for ensuring a rational and objective assessment of the projects. Such a situation is detrimental to a healthy development and growth of the e-governance sector.
- **Large National Action Plan ahead:** The National Action Plan on e-governance has an ambitious outlay of over Rs.12,000 crores involving public and private investments over the next four years. A significant portion of the National Action Plan involves replication of successful projects across different geographical areas of the country. However, the absence of a framework for knowing what a successful project is can severely handicap such replication efforts and also may result in misdirection of the scarce resources.
- **Canalizing ongoing efforts in the right direction:** As mentioned in 1.1 above, a lot of projects are already in different stages of implementation. It is desirable that a set of instruments is available to the administrators of those projects to appreciate the various attributes of a good e-governance project, apply midcourse corrections, where needed, and steer these projects in the right direction.
- **Facilitate funding agencies to take a rational view:** The National Action Plan involves significant private investments flowing into the e-governance sector. These funding agencies which could be banks, financial institutions or multilateral funding agencies would like to be assured that the resources would go into projects that have already been rated high as per a rational framework or can be appraised in terms of a widely accepted framework.

18.1.2 Objectives of an Assessment Framework

In the context of the need for an e-Governance Assessment Framework as described in section 1 above, the following specific objectives are formulated for the proposed Framework:

- To assess whether and to what extent a given e-Governance project has the characteristics of a good e-governance project delivering "Value" to stakeholders.
- To guide in funding of e-governance projects at various stages of their life-cycle (newly starting, roll-out, scaling up, replication)
- To provide guidelines for mid-term assessment of ongoing initiatives, so that mid-course corrections, if any, can be applied

- To provide guidelines for shaping future e-governance projects
- To provide material for e-governance training programs
- To enhance the trust and confidence of stakeholders by enabling creation of a knowledgebase of all e-Governance projects rated as per a trusted framework.

18.1.3 Categories of Projects

The variety, scope and size of e-Governance projects are very large. It is not possible to attempt to create a framework that is applicable to all possible projects. It is therefore proposed to confine the current exercise to the projects falling in the following four categories:

- Government to Citizen in Urban Environment (G2C- U)
- Government to Citizen in Rural Environment (G2C- R)
- Government to Business (G2B)
- Government to Government (G2G)

The projects can further be categorized on the basis of the investments made. The following table brings out the limits for categorization in respect of Pilot Projects and Rolled-out Projects separately.

The investments could be by the public or private sectors. In terms of priorities, it is desirable to focus the initial efforts on the large projects.

Category of Project	Pilot Project	Rolled - out Project
Small	< Rs.3 Cr	< Rs.10 cr
Medium	Rs.3 to 10 cr	Rs.10 to 50 cr
Large	> Rs.10 cr	> Rs.50 cr

18.1.4 Categories of frameworks

A very large number of parameters and attributes will have to be considered and assessed in order to decide the overall rating of an e-Governance project as detailed in Section 5. This would involve considerable resources to be invested. However, there are several occasions where it is not possible to invest such time and resource in administering the elaborate instruments. Keeping this in view, it is proposed to develop two tiers of instruments, the first tier for a summary assessment (SA) of the project and the second tier for a detailed assessment (DA). This requirement, together with the four-category classification of e-Governance Projects mentioned in Section 3 would lead to the need for developing eight instruments as mentioned below:

(a) Frameworks for Summary Assessment (SA)

4.1.1.	SA-G2C-U	Instrument for Summary Assessment framework for Government to Citizen, Urban Projects
4.1.2.	SA-G2C-R	Instrument for Summary Assessment framework for Government to Citizen, Rural Projects
4.1.3.	SA-G2B	Instrument for Summary Assessment framework for Government to Business Projects
4.1.4.	SA-G2G	Instrument for Summary Assessment framework for Government to Government Projects

(b) Frameworks for Detailed Assessment (DA)

4.2.1.	DA-G2C-U	Instrument for Detailed Assessment framework for Government to Citizen, Urban Projects
4.2.2.	DA-G2C-R	Instrument for Detailed Assessment framework for Government to Citizen, Rural Projects

4.2.3.	DA-G2B	Instrument for Detailed Assessment framework for Government to Business Projects
4.2.4.	DA-G2G	Instrument for Detailed Assessment framework for Government to Government Projects

The administration of the summary assessment instruments may be completed typically in 2 to 3 working days for single location projects, and 3 to 5 working days for multi-location projects, depending on the size of the project. The administration of the detailed instrument could take from 4 to 6 weeks depending on the size and complexity of the project.

18.1.5 Attributes to be Assessed

It is desirable that the frameworks developed are comprehensive, holistic and above all meet the objectives for which they have been designed. Essentially, the EAF should provide authentic and unambiguous answers to questions like the following:

a) How far has the Project succeeded in achieving its purpose and objectives?
b) Has the Project been designed and developed with all the technological features that are elegant and conform to widely accepted architectures and standards?
c) Is the Project sustainable over long periods of time, with or without the motive force that initiated the Project?
d) Is the Project cost-effective in terms of return on investment or in terms of cost per transaction?
e) Is the Project replicable in other geographies?

The various attributes required to be evaluated / rated in order to find reliable answers to the above 5 questions are given below. In all the tables, the columns 'Applicable to Tier' specify the applicability of the attribute to the tier of assessment (Summary Assessment: SA, Detailed Assessment: DA), and the columns 'Applicable to Category' specify the category of project (G2C-R, G2C-U, G2G, G-B, or All).

18.2 Service-Orientation

The attributes of the project, to be measured to assess the service orientation are grouped under three broad sub-groups namely: Efficiency, User-convenience, and Citizen- centricity. These are presented in the following tables.

18.2.1 Efficiency Attributes

	Attribute	Description and Measurement	Applicability	
			Assessment Tier	Project Category
1.	Speed of delivery of service	Measure this in days/hours/minutes and give a score between 0-5 based on the difference in speed before and after the project	SA, DA	All
2.	Compliance to committed service time frame	Measure the % of compliance and score: 1 for 1-20%, 2 for 21-40%, 3 for 41-60%, 4 for 61-80%, and 5 for 81-100%	SA, DA	All
3.	Quality of Service	User perception of Service Quality based on Location ambience, Staff courtesy, Display of information etc. (Score 0 for poor and 5 for excellent)	DA	All

4.	Simplicity of user actions required for obtaining the service	Give a score between 0-5 based on the differences in ease between the before and after improvements - forms, attachments, number of visits	DA	All
5.	% users benefited through e-Service compared to conventional channels	Give scores as 1 for 1-20%, 2 for 21-40%, 3 for 41-60%, 4 for 61-80%, and 5 for 81-100%	SA, DA	All
6.	(% Socially and economically backward) users benefited through e-Service	Give scores as 1 for 1-20%, 2 for 21-40%, 3 for 41-60%, 4 for 61-80%, and 5 for 81-100%	SA, DA	G2C-R

18.2.2 User-convenience Attributes

	Attribute	Description	Applicability	
			Assessment Tier	Project Category
I.	Ease of access to the service	How convenient is the location of the nearest service delivery point (0-5 scale)	SA, DA	All
2.	User independence of time : (24 x 7 availability)	How convenient is the time of service delivery operations (0-5 scale)	DA	All
3.	Single window access to several services	Extent to which the project offers all related services-end to end (0-5 scale)	DA	All
4.	Integrated services enabling access to several agencies through one request	Extent to which government services processing by several] requiring departments are offered in an integrated manner through the delivery stations (0-5 scale)	DA	All
5.	Mechanisms for problem resolution and exception handling	Observe how smoothly exceptions are handled and whether alternative processes exist in case of serious problems (0-5)	DA	All
6.	Suitability of service locations to socially and economically backward users	Observe the degree of suitability of the location to the socially and economically backward groups. Give a score of 5 if no inhibitions at all in using.(0-5)	DA, SA	G2C-R

18.2.3 Citizen-centricity Attributes

	Attribute	Description and Measurement	Applicability	
			Assessment Tier	Project Category
I.	Degree of alignment of service design to citizen's requirement	Extent of user requirements covered in the service design (0-5)	SA, DA	All
2.	Grouping of services around user's requirements and behavior patterns	Observe the grouping of services the extent to which they are in line with user's behavior pattern (0-5)	DA	All
3.	user interfaces in local language(s)	Extent of use of local language in user interfaces (0-5)	SA, DA	All

4.	New Services and their relevance to citizens	Extent of citizen-centric new services offered - other than the conventional services offered earlier (0-5)	DA	All
5.	Reduction of visits to high level government offices	Percentage reduction in user visits to high level offices (district / taluka) to complete the transaction	SA,DA	G2C-R
6.	Knowledge of Service provider on the services offered	Extent to which the staff of service provider at service delivery station is familiar with the services packaged for different user groups	DA	G2C-R

18.3 Technology

The technology and its robustness are important for a project's performance. The attributes measuring technological base are its architecture, compliance to standards, inter-operability, security, scalability, and reliability.

18.3.1 Architecture Attributes

	Attribute	Description and Measurement	Applicability	
			Assessment Tier	Project Category
I.	Comprehensiveness of the architecture to meet the needs of the project	Is the configuration adequate to handle all the services? Score low if it is under-designed or over-designed (0-5)	SA, DA	All
2.	Conformance of the architecture to National / International architectures	Extent to which the architecture is in line with the national and International architectures (0-5)	DA	All
3.	Mechanism in place for enforcing the compliance to architecture	Is there a system in place for conducting third party audit of the systems to elicit conformance / continued conformance to the architecture originally designed ?	DA	All
4.	Provisions for Inter-operability	Does the system inter-operate with the systems of any other department? If not, does the design support such inter-operability ? 0-5	DA	All
5.	Extent of the use of Open Source Software Systems	Based on the use of OSS: for OS, DBMS, Web-server etc (0-5)	DA	All

18.3.2 Attributes on Standards

	Attribute	Description and Measurement	Applicability	
			Assessment Tier	Project Category
I.	Extent of compliance of the project to open standards	Based on use of open standards like TCP/IP, HTTP, CORBA, DCOM, ODBC (O-5)	DA	All
2.	Mechanism in place for enforcing the compliance to standards	Is there a system in place for conducting third party audit of the systems to elicit conformance / continued conformance to he standards ?	DA	All

3.	Extent of design and adoption of metadata standards	Is the system based on the use of metadata standards like XML etc ? (O-5)	DA	All

18.3.3 Security Attributes

	Attribute	Description and Measurement	Applicability	
			Assessment Tier	Project Category
I.	Design of security architecture and policy	Does the system security design conform to BS 7799? (Score -5) Or is there a security policy in place? (4 to 0)	DA	All
2.	Extent of compliance to security architecture	Degree of compliance to security architecture/ policy as assessed by a third party (0-5)	DA	All
3.	Mechanism in place for enforcing the compliance to security policy	Is there a system in place for conducting third party audit of the systems to elicit conformance / continued conformance to the standards ? (Yes -5, No- 0)	DA	All
4.	Mechanism in place for the users to make secure electronic	Yes 5; No -0	SA, DA	All

18.3.4 Scalability Attributes

	Attribute	Description and Measurement	Applicability	
			Assessment Tier	Project Category
I.	Extent to which the design permits scalability	Based on the APIs available and their documentation (0-5)	DA	All
2.	Degree of scalability of project to cover target users completely	Based on provisions to handle large number of users and transactions without sacrificing response (0-5)	SA, DA	All
3.	Extent of scope for incorporating enhanced hardware interfaces	Based on the extent to which both hardware and software designs permit integration of new devices (0-5)	DA	All
4.	Extent of scope to work with alternate power and connectivity solutions	Based on the design of system which permits use of alternate energy and communication systems (0-5)	DA	All

18.3.5 Reliability related Attributes

	Attribute	Description and Measurement	Applicability	
			Assessment Tier	Project Category
I.	Degree of Availability	High degree of availability: 99.99% through disaster recovery systems and alternative channels, gets a score of 5 (0-5 scale)	SA, DA	All
2.	Degree of Accuracy	System that produces highly accurate results gets a score of 5. (Assessment to be based on third party audits and error logs of the system.)	DA	All

3.	Consistency of Response times	The consistency with which system offers reasonable response times response to be assessed from the system logs.	DA	All
4	Availability of SLA (Service Level Agreement)	Are the operational contracts based on a system of SLAs? Yes -5; No-0.	SA, DA	All
5.	Availability of alternative service delivery channels in case of system breakdowns	Extent to which the users can depend on the system's response in case of breakdowns (power, connectivity, hardware, software).	SA, DA	G2C-R

18.4 Sustainability

The sustainability of a project depends on the organizational sustainability, commercial sustainability, and legal sustainability. The attributes measuring these are given in the following tables :

18.4.1 Organizational Sustainability Attributes

	Attribute	Description and Measurement	Applicability	
			Assessment Tier	Project Category
I.	Existence and functioning of an organizational structure for managing the project	Whether created by reforming the conventional structure and is functioning effectively (O-5)	SA, DA	All
2.	Extent and adequacy of training imparted to employees of the organization	Based on the comfort levels of employees in offering service through new system (O-5)	DA	All
3.	Role clarity and degree of employee-buy-in (Change management)	If no ambiguity exists on the roles to be played by employees in the changed environment, 5 (O-5)	SA, DA	All
4.	Degree of involvement of employees in project design, development & implementation	Based on the degree of sense of ownership of the project by the government employees (O-5)	DA	All
5.	Continuity of top champions of the project for 3-5 years	Score I for each year of continuity; Less than one year (O-5)	SA, DA	All
6.	Existence and effectiveness of User Groups and Service Reviews	Based on the existence and effectiveness of a system of reviewing the system operations periodically, incorporating user feedback (O-5)	SA, DA	All

18.4.2 Commercial Sustainability Attributes

	Attribute	Description and Measurement	Applicability	
			Assessment Tier	Project Category
I.	Amenability of Service Delivery through PPP mode	Based on the degree to which the service is amenable for private participation (0-5)	SA, DA	All
2.	Strength of PPP arrangement (if PPP)	Based on effectiveness with which the private partner is executing the project (0-5)	SA, DA	All

3.	Stability, Expertise, and commitment of Service Delivery agents (if PPP?)	Based on the industry standing of the private agency and the types of projects handled by them (0-5)	DA	All
4.	Collection of user charges	Score 5, if the charges provide good stream of revenue adequate to ensure financial sustainability (0-5)	SA, DA	All
5.	Arrangements to ensure availability of service during user convenient time slots	Score 5 if power supply, and connectivity are available during the prime time slots (0-5)	SA, DA	All
6.	Period of continuous functioning of the project after launch without showing symptoms of decline through reduced number of transactions	Score 5 if the project functions for 3 years or more after launch without decline and with growth. Score MINUS I0 if the project has stopped functioning within 3 years of launch and MINUS 5 if the numbers show a decline.	SA, DA	All
7.	Economic benefit to the users in the rural areas	Extent to which the services provide economic benefit to the citizens in rural areas	SA, DA	G2C-R

18.4.3 Legal Sustainability Attributes

	Attribute	Description and Measurement	Applicability	
			Assessment Tier	Project Category
I.	Extent of Business Process Re-engineering undertaken	Extent to which the processes are simplified taking advantages of ICT (0-5)	SA, DA	All
2.	Amendments carried out to Act (s) and Rules relating to provision of the e-services	Extent to which age-old rules are modified to facilitate improved service delivery covering all services envisaged under the project (0-5)	DA	All

18.5 Cost-effectiveness

The cost-effectiveness will have to be assessed from the view point of users (citizens, enterprises), service providers and the government.

18.5.1 Cost Effectiveness Attributes

	Attribute	Description and Measurement	Applicability	
			Assessment Tier	Project Category
I.	Extent of reduction of direct cost to user compared to earlier system	Estimate the percentage reduction in direct cost like travel cost and give a score between O-5	SA, DA	All
2.	Extent of reduction of indirect cost involved in repeated visits	Estimate the % reduction in indirect cost like cost of repeated visits and give a score (O-5)	DA	All
3.	Extent of cost reduction to government	Based on reduction communication costs, staff costs etc. (O-5)	DA	All

4.	Enhanced revenue/benefit to the government	Based on the increase in revenues and benefits to government (O-5)	SA, DA	All
5.	Degree of reduction in corruption	Based on citizens perception on corruption with new system: O-5 (5 if high reduction)	SA, DA	All
6.	Recovery of Capital cost	If provision is made for complete recovery score as 5 (O-5)	DA	All
?.	If PPP, Commercial viability for Private Partner	If high commercial viability for Private partner 5 (O-5)	DA	All

18.6 Replicability

The factors contributing to replicability of e-Governance project are: functional replicability, technological replicability, and commercial replicability. The attributes measuring each of these factors are given in the tables below:

18.6.1 Functional Replicability Attributes

	Attribute	Description and Measurement	Applicability	
			Assessment Tier	Project Category
I.	Degree of generic processes introduced compared to processes which are specific to the project geography	Extent to which the project addresses issues not specific to geography (state / district etc.); can be implemented anywhere in the country (O-5)	DA	All
2.	Degree of resemblance/ alignment of the application software to 'Product' than to a 'bespoke software'	Extent to which a product has been and/or can be developed out of the project (O-5)	DA	All

18.6.2 Technological Replicability Attributes

	Attribute	Description and Measurement	Applicability	
			Assessment Tier	Project Category
I.	Multiple Platform Feasibility	Extent of feasibility of deployment Application software on multiple platforms (0-5)	DA	All
2.	Ease of installation of the systems in new locations	Extent of ease of installation - score 5 if application is browser based (0-5)	DA	All
3.	Extent of parameterization for customization	Extent to which it is customizable through parameters only (not through additional programming) (0-5)	DA	All
4.	Feasibility of replication only few modules of the system	Extent to which system permits use of few sub-systems independently (like online application) 0-5	DA	All
5.	Quality of project documentation	Based on availability of system documentation in standard format (0-5)	SA, DA	All
6.	Quality of user manuals	0-5 Based on how well the user instructions are presented	SA, DA	All

18.6.3 Commercial Replicability Attributes

	Attribute	Description and Measurement	Applicability	
			Assessment Tier	Project Category
I.	Replication arrangement with Application developer	Whether the commercial arrangement with the developer / PPP partner permits replication - Yes / No (5 or 0)	SA, DA	All
2.	Commercial viability	Whether the transaction costs and other commercial terms are attractive enough to induce replication : Yes / No (5 or 0)	DA	All
3.	Marketing strength for replication	Is there a mechanism in place for marketing' the project and implementing it in other geographies on commercial basis Yes / No (5 or 0)	DA	All

18.7 Weightages to be assigned to different Attributes

All the attributes mentioned in Section 5 are not relevant to each e-Governance Project to be assessed. Even if relevant, their weightages could be different in the context of different projects. For example, while service orientation carries a heavy weightage in citizen centric projects, technology and replicability carry a higher weightage in G2G Projects aimed at enhancing internal efficiency and effectiveness of Government Organizations. The following matrix gives the set of weightages to the different parameters in each project category:

Attribute Class	Project Category			
	G2C-R	G2C-U	G2B	G2G
Service Orientation	40	40	30	20
Technology	20	20	20	20
Sustainability	20	20	20	20
Cost-effectiveness	10	10	20	20
Replicability	10	10	10	20

18.8 Instruments for Assessments

As presented in section 4, each type of assessment requires a different instrument for collection of data and its analysis. These instruments can be developed using the attribute tables presented above, as follows:

- Select the attributes applicable to the type of assessment, using the columns 'Applicability', from the tables in section 5. For example, instruments for simple assessment of a G2C Rural project will have only those attributes which are marked 'SA' in the 'Applicability : Assessment' column; and those which have "All" as well as G2C-R in the 'Applicability : Project" column.
- Develop questions to collect the data for the selected attributes. Each attribute is required to be scored on a scale of 0-5.
- In addition, each instrument should have questions to collect data on the background of projects and respondents as given in the sections below. Such background data is required to perform assessments based on the various project and respondent attributes.

18.8.1 Project Background

The primary set of data required to evaluate all types of projects is the project background data, which may be categorized as:

Project Context, Project Objectives, and Project Services

Detailed elements of these three categories of data sets are given in tables below. Sources of such data are mainly the project documents.

18.8.2 Project Context

The project context helps us to categorize the project and analyze its data from the various aspects. The table below gives the details of data elements that capture the project context.

Item	Remark
State	
Sector	Health, Education, Industry, Transport, …
Target population	
Demographic profile	Composition of the population
Project Domain	G-CU, G-CR, G-B, G-G
Target group / Expected beneficiaries	All citizens, women, children, tribal, NGO, ..
Stakeholders of the project	Government Departments, Citizens, Enterprises
Stage of the project	Pilot, Phase-I, Roll out, Enhancement, etc.
Scale of the project	Small Pilot, Medium Pilot, Large Pilot, Small Regular, Medium Regulat, Large Regular
Implementation mechanism	In-house, Private, Govt. Agency, PPP
Type of access to Services	Portal, Kiosk, Delivery station, Office Desk
Type of Service Delivery Contract	BOO, BOOT, Govt. own- private-run, etc.
Backgrounds & Tenures of Project managers	Project Managers at different phases
Sources of Funds and Amounts	One-time, recurring (Loans, Grants)
Sharing of Expenses	Between Govt., and Service Provider
Sharing of Revenues	Between Govt., and Service Provider
Ownership of hardware & system software	Government, Service Provider
Ownership of application software	Who owns the IP? (Govt, Service developer)

18.8.3 Project Objectives

Mostly, e-Governance projects are designed with some of the following objectives:

1. Minimizing distance to access
2. Extending access to un-served groups
3. Introducing transparency
4. Simplifying transaction procedures
5. Minimizing cost to citizens
6. Minimizing cost to government (internal efficiency)
7. Increasing the government revenue
8. Improving the time to transact (citizen, government)
9. Offering new services
10. Modernization / adoption of Best Practices

Information on the project objectives may be collected in the following table:

Objective	Importance (Rank)	Remarks

Objectives and their rank order are useful in performing a detailed analysis.

18.8.4 Project Services

Each project offers several services to achieve the stipulated objectives. To evaluate the benefits perceived by stakeholders, it is necessary to collect all the categories of services and the specific services in each category. Subsequently, detailed feedback may be obtained on each of the services. Data may be collected in the following format:

Service Category	Remarks
On-line transaction processing (all stages, some stages)	Bill Payments, Reservations, Applications (Licenses, Ration Cards, Pensions), Status report on applications, Returns filing, Results, Counseling
Information dissemination	Forms, Rules, News, Market prices, Tenders, etc.

18.9 Respondent Background

The following data on the profile of respondents (all stakeholders) may be collected for each respondent to perform detailed segment wise analysis of different target groups:

Item	Remarks
Stakeholder role	Citizen, Service Provider, Government Employee
Gender	
Caste	Only if needed
Religion	Only if needed
Age group	
Income Group	
Education	
Occupation	

18.10 Model Templates for Assessment

A set of model templates for the assessments, in the spreadsheet format, is appended to this report (Annexures 1 to 8). The attributes appropriate to each category are incorporated in each spreadsheet and the weightages are also built into the spreadsheet as formulae. This enables generation of the composite score automatic as soon as the responses to all the questions are made on a scale of 0-5. This ensures ease of administration of the instruments besides uniformity in measurement of different projects. Exhibits 1 to 4 provide sample assessments made using the templates.

18.11 Assessment Methodology

The evaluations are to be conducted completely under free atmosphere. This process should not be handed over to the project management staff or the service providers. There must be total autonomy to sample design, selection of respondents and locations. Similarly, there must be total freedom to administer the questionnaires. Each project to be assessed must give consent and fully cooperate in conducting the study as per the above terms.

Standard sampling techniques shall be adopted in arriving at the size of the sample, the locations and respondents.

The assessment should be conducted in two steps: The Summary Assessment and the Detailed Assessment.

18.11.1 Summary Assessment

It is suggested that summary assessment be conducted on a small sample. It should start with collection of data on the project (and similar projects) from secondary sources to facilitate development of a broad framework for evaluation. The study should include interviews and administration of questionnaires on a small sample of respondents (of a representative sample of stakeholders). Summary Assessment should offer broad insights into the ground realities of the project and provide inputs to sharpen the understanding of the project objectives, identification of stakeholders, control groups, affected groups, etc., and help us refine the data collection instruments. Authorizations for conducting the interviews and collection of data should be obtained during this stage from the concerned authorities. To a large extent, the data collection should be done in a natural environment, preferably without giving prior notice to the concerned parties so that it is not biased.

18.11.2 Detailed Assessment

The detailed study should be based on a scientific sampling plan, which is refined by the exploratory study. The sampling plan should detail out the location wise and the type wise number of stakeholders to be surveyed.

The sampling plan must include all stake holders and representative geographic locations. It should include a reasonable sample size (about 20%) of those who are not users of the e- governance project, i.e., control groups, and those who are affected by the new system. Separate instruments may be developed for each group. The instruments for control group will have only those attributes which are in the service orientation class.

18.11.3 Computing the Assessment Scores

A typical instrument for assessment would have a large number of attributes grouped under the classes namely, Service orientation, Technology, Sustainability, Cost-effectiveness, and Replicability. As presented in section 5, each attribute in the instrument has to be given a score between zero and five. At present we recommend equal weight to each attribute in a class. Therefore depending on the number of attributes in the class, the total possible score for that class would vary. For example, if the service orientation class has 14 attributes, it would give a maximum possible score of 14*5 = 70.

The score obtained for each attribute class should be given a specified weightage as per the scheme presented in the section 6 (for a G2C project, the weightage given to service orientation class is 40).

If the total score obtained for the 14 attributes of service-orientation class, for example is 35 (against a total of 70), to compute the assessment score for this segment, we divide the score obtained by 70 and multiply it by 40. The assessment score for 'service orientation' would therefore be (35 / 70) * 40 = 20.

Perform the similar computations for all other classes, using the weightages given herein.

18.11.4 Interpreting Assessment Scores

The total score obtained by a project clearly gives an overall assessment of the project. However it is important to assess a project based on the scores obtained in the individual segments. For example, a project may get an overall high assessment score, but it may be weak in sustainability segment (like sample G2B project: 12.86 out of 20). It is important to identify the attributes on which the project has scored poorly (or highly) to draw lessons for the future projects. For example, this project is weak in 'continuity of top champions', 'existence of user groups', and strength of PPP arrangement.

The following general guidelines are provided for interpreting the assessment scores of individual projects

A prima facie assessment of the strength of a project for a further investment decision, for expansion or for replication can be based on the yardstick given in the table below:

No.	Score Range	Category	Remarks
1.	70 and above	**Extremely Good**	Qualifies for further investment of resources / replication
2.	50 to 69	**Good**	Scope for marginal improvements
3.	40 to 49	**Satisfactory**	Amenable to improvements through course correction and gap filling
4.	Below 40	**Poor**	Not worthy of pursuing further

18.12 Criteria for selection of agencies for conducting the assessment

Agencies performing Assessments must satisfy the following criteria:

1. Have experience in conducting Market Research
2. Have familiarity with e-Governance projects
3. Should be disinterested and neutral. (e.g. Academic Institutions, research establishments, and consulting organizations)
4. Should be able to employ investigators who understand the regional issues and local language
5. Should be able to employ investigators who should be able to broadly understand information technology and e-governance issues

Examples of such organizations are:

1. Research centers of Indian Institutes of Management
2. Management schools / departments of Indian Institutes of Technology
3. Indian Institutes of Information Technology (IIITs)
4. IRMA, MICA, Management Institutes which have e-Governance focus
5. Departments of Universities with Management / E-Governance curriculum
6. ORG-MARG, Mudra
7. Public Affairs Council (Bangalore)
8. Institutes engaged in applied research in Economic and Social development

The selected agencies should be invited for a one-day workshop by DIT, through which they are briefed on the e-Governance projects and the assessment objectives. The first half of the workshop may cover some successful and not so successful projects from each category (G2CR, G2CU, G2B and G2G), so that the agency representatives strengthen their understanding of e-Governance projects. The second part of the workshop should cover the assessment methodology, clarifying all the attributes and their scoring.

"The assessment agents should agree to:

1. Develop questionnaires based on assessment templates
2. Employ and train investigators
3. Conduct field surveys
4. Summarize and draw conclusions
5. Present conclusions including sharing of source data"

18.13 Summary and Conclusion

The above methodology has been designed to serve many objectives spelt out in the first Section. Two levels of assessments (a quick assessment and an in depth assessment) are outlined to serve the important purpose of identifying those e-Governance projects which should be replicated in other States and locations.

Two important attributes of a project would determine whether it should be selected for replication:

- Value that the project delivers to its primary clients and also to the many other stakeholders that are involved in delivering the government service.
- "Adaptability of the Technology architecture to different contexts"

Value needs to be measured in concrete terms as has been proposed in this methodology. However, given the variety of contexts in which e-Governance applications are built, it is impossible to monetize the value. Whereas cost reduction, an increase in revenue are monetizable; reduction in corruption, increase in transparency or even improvements in service levels are not easily monetizable.

Judgment is likely to play a significant role in trading off specific benefits delivered across different dimensions to arrive at an overall value for purposes of comparison across projects. Through such comparison it would be possible to select those projects which seem to deliver the maximum value. A committee of experts can be used to exercise this judgment. The methodology presented here makes it easier to exercise the judgment by presenting an unbiased measurement of benefits on dimensions that are perceived to be important for a specific application.

19. Guidelines for usage of Digital Signatures in e-Governance

19.1 Introduction to Digital Signatures

The Department of Information Technology, Government of India, has felt it necessary to create a rational framework for assessing e-Governance projects on various dimensions. The justification for creation and use of such a framework is given below:

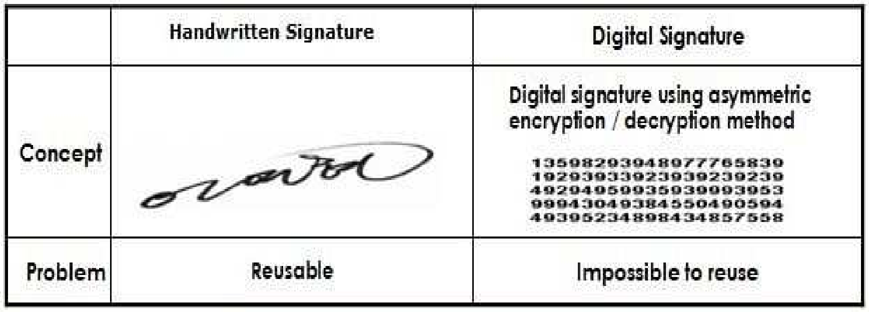
A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document, and to ensure that the original content of the message or document that has been sent is unchanged. Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time-stamped. A digital signature can be used with any kind of message, whether it is encrypted or plaintext. Thus Digital Signatures provide the following three features:-

- **Authentication-** Digital signatures are used to authenticate the source of messages. The ownership of a digital signature key is bound to a specific user and thus a valid signature shows that the message was sent by that user.
- **Integrity -** In many scenarios, the sender and receiver of a message need assurance that the message has not been altered during transmission. Digital Signatures provide this feature by using cryptographic message digest functions (discussed in detail in section 4.4).
- **Non Repudiation -** Digital signatures ensure that the sender who has signed the information cannot at a later time deny having signed it.

19.2 Digital Signature Versus Handwritten Signatures

A handwritten signature scanned and digitally attached with a document does not qualify as a Digital Signature. A Digital Signature is a combination of 0 & 1s created using crypto algorithms.

An ink signature can be easily replicated from one document to another by copying the image manually or electronically. Digital Signatures cryptographically bind an electronic identity to an electronic document and the digital signature cannot be copied to another document. Further, paper contracts often have the ink signature block on the last page, allowing previous pages to be replaced after the contract has been signed. Digital signatures on the other hand compute the hash or digest of the complete document and a change of even one bit in the previous pages of the document will make the digital signature verification fail. As can be seen in the underlying figure, a Digital Signature is a string of bits appended to a document. The size of a digital signature depends on the Hash function like SHA 1 I SHA2 etc used to create the message digest and the signing key. It is usually a few bytes.



	Handwritten Signature	Digital Signature
Concept		Digital signature using asymmetric encryption / decryption method 13598293948077765839 19293933923939239239 49294959935939993953 99943049384550490594 49395234898434857558
Problem	Reusable	Impossible to reuse

19.3 Difference between Electronic Signatures and Digital signatures

An electronic signature means authentication of an electronic record by a subscriber by means of electronic techniques. An Amendment to IT Act in 2008 has introduced the term electronic signatures. The implication of this Amendment is that it has helped to broaden the scope of the IT Act to include new techniques as and when technology becomes available for signing electronic records apart from Digital Signatures.

19.4 Overview of how Digital Signatures work

The Digital Signatures require a key pair (asymmetric key pairs, mathematically related large numbers) called the Public and Private Keys. Just as physical keys are used for locking and unlocking, in cryptography, the equivalent functions are encryption and decryption. The private key is kept confidential with the owner usually on a secure media like crypto smart card or crypto token. The public key is shared with everyone. Information encrypted by a private key can only be decrypted using the corresponding public key.

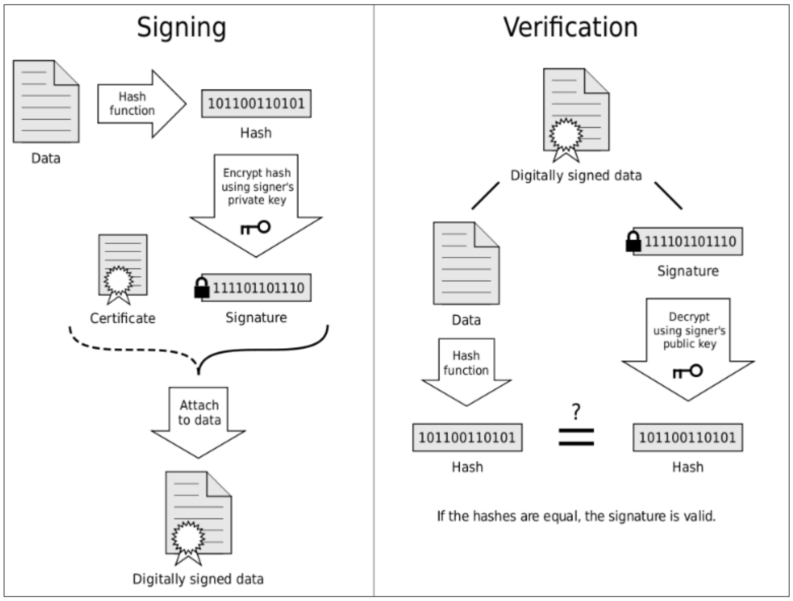
In order to digitally sign an electronic document, the sender uses his/her Private Key. In order to verify the digital signature, the recipient uses the sender's Public Key.

Let us understand how the Digital Signatures work based on an example. Assume you are going to send the draft of a contract to your lawyer in another town. You want to give your lawyer the assurance that it was unchanged from what you had sent and that it is really from you.

1. You copy-and-paste the contract into an e-mail note. Get electronic form of a document (e.g. Word or PDF file)
2. Using special software, you obtain a message hash (fixed size bit string) of the contract.
3. You then use your private key to encrypt the hash.
4. The encrypted hash becomes your digital signature of the contract and is appended to the contract.

At the other end, your lawyer receives the message.

1. To make sure the contract is intact and from you, your lawyer generates a hash of the received contract.
2. Your lawyer then uses your public key to decrypt the Digital Signature received with the contract.
3. If the hash generated from the Digital Signature matches the one generated in Step 1, the integrity of the received contract is verified.



Note: Message digest, also known as the hash of a message, is a small piece of data that results by applying a particular mathematical calculation (hashing function) on the message. Two properties of message digests to note: (i) a small alteration in the original message would cause a big change in the message digest; (ii) derivation of the original message is not possible from the message digest. The hash produced from these functions is a fixed length bit string. For example: - The widely used message digest function SHA -1 generates a 160 bit hash whereas the SHA-2 function generates 256 bit hash as output. The usage of MD5 is to be discontinued by the Certifying Authorities as per the Amendment to the Rules of the IT Act published in 2009.

19.5 Legal Validity of Digital Signatures

The Information Technology Act 2000 came into effect from October 17, 2000. One of the primary objectives of the Information Technology Act of 2000 was to promote the use of Digital Signatures for authentication in e-commerce & e-Governance. Towards facilitating this, the office of Controller of Certifying Authorities (CCA) was set up in 2000. The CCA licenses Certifying Authorities (CAs) to issue Digital Signature Certificates (DSC) under the IT Act 2000. The standards and practices to be followed were defined in the Rules and Regulations under the Act and the Guidelines that are issued by CCA from time to time. The Root Certifying Authority of India (RCAI) was set up by the CCA to serve as the root of trust in the hierarchical Public Key Infrastructure (PKI) model that has been set up in the country. The RCAI with its self-signed Root Certificate issues Public Key Certificates to the licensed CAs and these licensed CAs in turn issue DSCs to end users.

Section 5 of the Act gives legal recognition to digital signatures based on asymmetric cryptosystems. The digital signatures are now accepted at par with the handwritten signatures and the electronic documents that have been digitally signed are treated at par with the paper based documents.

An Amendment to IT Act in 2008 has introduced the term electronic signatures. The implication of this Amendment is that it has helped to broaden the scope of the IT Act to include other techniques for signing electronic records as and when technology becomes available.

19.6 Public Key Infrastructure in India

PKI is the acronym for Public Key Infrastructure. The technology is called Public Key cryptography because unlike earlier forms of cryptography it works with a pair of keys one of which is made public and the other is kept secret. One of the two keys may be used to encrypt information which can only be decrypted with the other key. The secret key is usually called the private key. Since anyone may obtain the public key, users may initiate secure communications without having to previously share a secret through some other medium with their correspondent. PKI is thus the underlying system needed to issue keys and certificates and to publish the public information. PKI is a combination of software, encryption technologies, and services that enable enterprises to protect the security of their communications and business transactions over networks by attaching so-called "digital signatures" to them.

The Office of the Controller of Certifying Authorities (CCA), has been established under the Information Technology (IT) Act 2000 for promoting trust in the electronic environment of India. The current PKI organization structure in India consists of the Controller of Certifying Authority as the apex body and as the Root Certifying Authority of India (RCAI)(as shown in the figure on PKI Heirarchy). The CCA is entrusted with the following responsibilities : -

- Licensing Certifying Authorities (CAs) under section 21 of the IT Act and exercising supervision over their activities.

- Controller of Certifying Authorities as the "Root" Authority certifies the technologies and practices of all the Certifying Authorities licensed to issue Digital Signature Certificates
- Certifying the public keys of the CAs, as Public Key Certificates (PKCs).
- Laying down the standards to be maintained by the CAs.
- Conflict resolution between the CAs
- Addressing the issues related to the licensing process including:
    - Approving the Certification Practice Statement (CPS);
    - Auditing the physical and technical infrastructure of the applicants through a panel of auditors maintained by the CCA.

The RCAI is responsible for issuing Public Key Certificates to Licensed Certifying Authorities (henceforth referred to as Certifying Authorities or CA). The CAs in turn are responsible for issuing Digital Signature Certificates to the end users. In order to facilitate greater flexibility to Certifying Authorities, the CCA has allowed the creation of sub-CAs. As per this model, a Certifying Authority can create a sub-CA to meet its business branding requirement. However the sub-CA will be part of the same legal entity as the CA.

The sub-CA model will be based on the following principles:

- The CAs must not have more than one level of sub-CA
- A sub-CA certificate issued by the CA is used for issuing end entity certificates
- A CA with sub-CA must necessarily issue end entity certificates only through its sub-CA. The only exception will be for code signing and time stamping certificates, which may directly be issued by the CA.

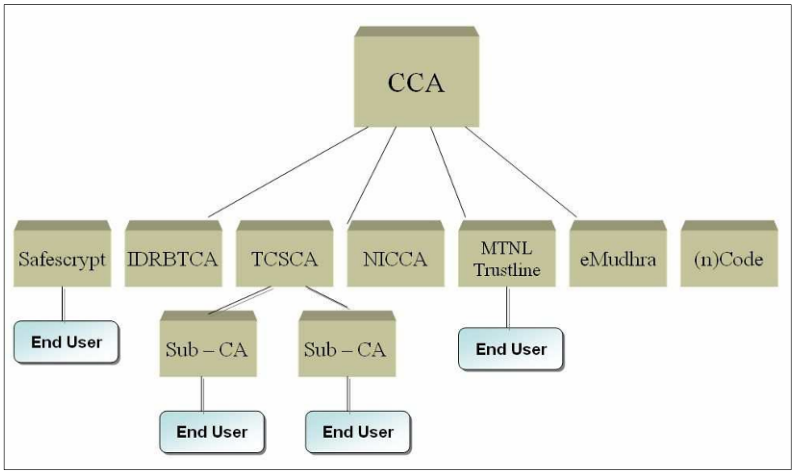


Figure: Overview of PKI Hierarchy in India

A Registration Authority (RA) acts as the verifier for the Certifying Authority before a Digital Signature Certificate is issued to a requestor. The Registration Authorities (RAs) process user requests, confirm their identities, and induct them into the user database.

The PKI structure (outlined in the Figure below) in India is the foundation for secure Internet applications which ensure authentic and private transactions that cannot be repudiated at a later time. Thus the CCA certifies the public keys of CAs using its own private key, which enables users in the cyberspace to verify that a given certificate is issued by a licensed CA. For this purpose it operates as the Root Certifying Authority of India (RCAI). CCA is the Root of the trust chain in India.

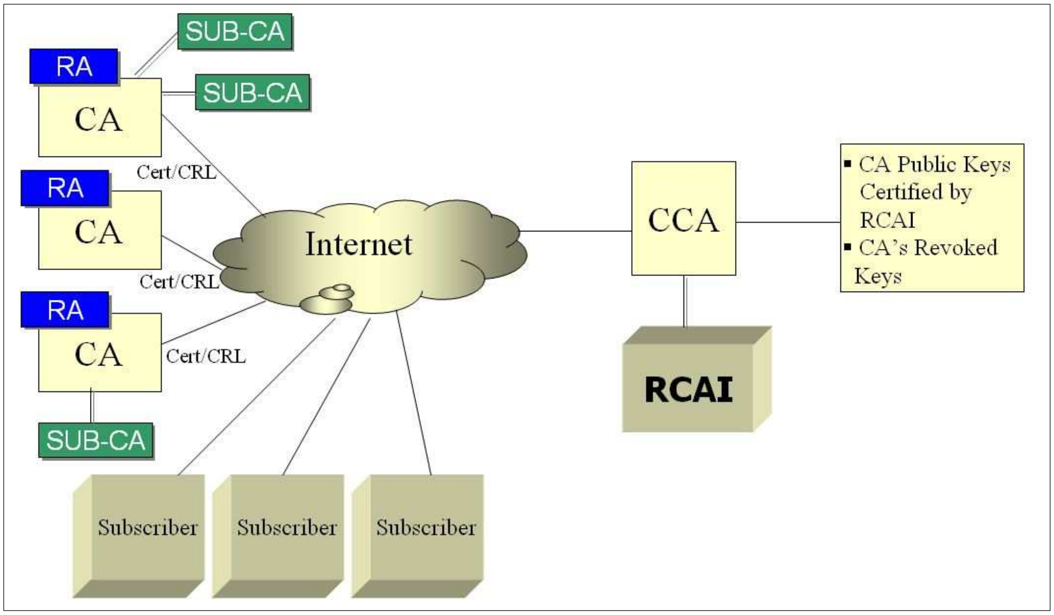


Figure: Overview of CCA Implementation of PKI as per the IT Act

In order to ensure interoperability between the Digital Signature Certificates issued by different CAs' in India, the CCA has come out with the "Interoperability Guidelines for Digital Signature Certificates issued under the Information Technology Act" (http://cca.gov.in/rw/pages/index.en.do). With these guidelines in place, the Digital Signature Certificate issued by one CA can be used across various e-Governance applications as the Interoperability guidelines have prescribed the formats, field and other aspects that will ensure interoperability. To know more about CCA kindly visit their website http://cca.gov.in/.

19.7 Digital Signature Certificates

Certificates serve as identity of an individual for a certain purpose, e.g. a driver's license identifies someone who can legally drive in a particular country. Likewise, a Digital Signature Certificate (DSC) can be presented electronically to prove your identity or your right to access information or services on the Internet.

A Digital Signature Certificate is an electronic document which uses a digital signature to bind together a public key with an identity - information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to the individual. Digital certificates are the digital equivalent (i.e. electronic format) of physical or paper certificates. Examples of physical certificates are driver's licenses, passports or membership cards.

Digital Signature Certificates are endorsed by a trusted authority empowered by law to issue them, known as the Certifying Authority or CA. The CA is responsible for vetting all applications for Digital Signature Certificates, and once satisfied, generates a Digital Certificate by digitally signing the Public key of the individual along with other information using its own Private key.

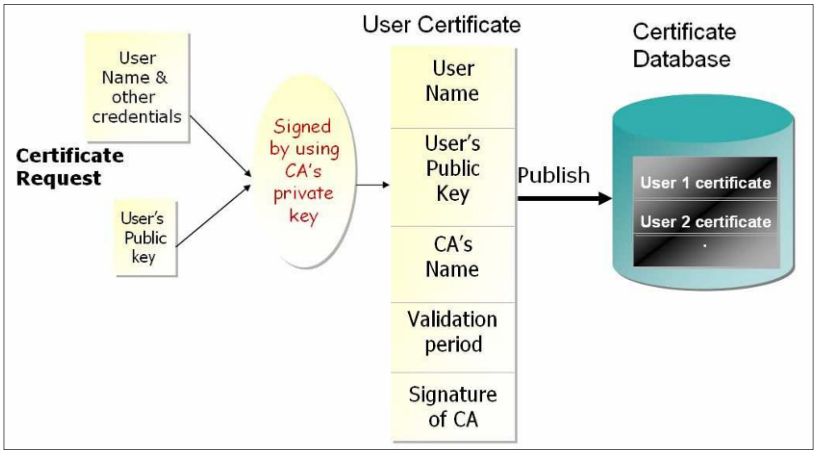


Figure: Overview of Digital Signature Certificate

19.8 Classes of Digital Signature Certificates

Depending upon the requirement of assurance level and usage of DSC the following are the classes of Digital
Signature Certificates

Class of DSC	Assurance Level	Applicability
Class 1	Class 1 certificates shall be issued to individuals/private subscribers. These certificates will confirm that user's name (or alias) and E-mail address form an unambiguous subject within the Certifying Authorities database.	This level provides a basic level of assurance relevant to environments where there are risks and consequences of data compromise, but they are not considered to be of major significance. This may include access to private information where the likelihood of malicious access is not high. It is assumed at this security level users are not likely to be malicious.
Class 2	These certificates will be issued for both business personnel and private individuals use. These certificates will confirm that the information in the application provided by the subscriber does not conflict with the information in well-recognized consumer databases.	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial.
Class 3	These certificate will be issued to individuals as well as organizations. As these are high assurance certificates, primarily intended for e-commerce applications, they shall be issued to individuals only on their personal (physical) appearance before the Certifying Authorities.	This level is relevant to environments where threats to data are high or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk.

19.9 Types of Digital Signature Certificates

The following table provides an overview of the different types of Digital Signature Certificates.

Type of Certificate	Description
Individual Digital Signature Certificates (Signing Certificates)	Individual Certificates serve to identify a person. It follows that the contents of this type of certificate include the full name and personal particulars of an individual. These certificates can be used for signing electronic documents and emails and implementing enhanced access control mechanisms for sensitive or valuable information.
Server Certificates	Server Certificates identify a server (computer). Hence, instead of a name of a person, server certificates contain the host name e.g. "https://nsdg.gov.in/ " or the IP address. Server certificates are used for 1 way or 2 way SSL to ensure secure communication of data over the network.
Encryption Certificates	Encryption Certificates are used to encrypt the message. The Encryption Certificates use the Public Key of the recipient to encrypt the data so as to ensure data confidentiality during transmission of the message. Separate certificates for signatures and for encryption are available from different CAs.

19.10 Certificate Revocation

Digital Signature Certificates are issued with a planned lifetime, which is defined through a validity start date and an explicit expiration date. A certificate may be issued with a validity of upto two years. Once issued, a Certificate is valid until its expiration date.

However, various circumstances may cause a certificate to become invalid prior to the expiration of the validity period. Such circumstances include change of name (for example, change the subject of a certificate due to an employee's change of name), change of association between subject and CA (for example, when an employee terminates employment with an organization), and compromise or suspected compromise of the corresponding private key. Under such circumstances, the issuing CA needs to revoke the certificate.

In case a Digital Signature Certificate is compromised, one should immediately contact the respective CA to initiate revocation. The CA will then put the certificate in the Certificate Revocation List. We need to have necessary processes in place defining the roles and responsibility of various government officials for the usage of Digital Signature and their revocation.

19.11 Certificate Revocation List (CRL)

A CRL is a list identifying revoked certificates, which is signed by a CA and made freely available at a public distribution point. The CRL has a limited validity period, and updated versions of the CRL are published when the previous CRL's validity period expires. Before relying on a signature the CRL should also be checked to ensure that the corresponding DSC has not been revoked.

19.12 Digital Signature Certificate Verification

Digital Signature Certificates are verified using a Chain of trust. The trust anchor for the Digital Certificate is the Root Certifying Authority (CCA in India). A root certificate is the top-most certificate of the hierarchy, the private key of which is used to "sign" other certificates. All certificates immediately below the root certificate inherit the trustworthiness of the root certificate. Certificates further down the tree also depend on the trustworthiness of the intermediates (often known as "subordinate certification authorities").

The Digital Certificate verification process is a recursive process in which the program verifying the end user certificate verifies the validity of the certificate of the issuing authority until it finds a valid certificate of a trusted party. On successful verification of the trusted party Certificate, the Digital Certificate verification stops. In case a trusted party Certificate is not found by the program, the Digital Certificate verification process ends in failure.

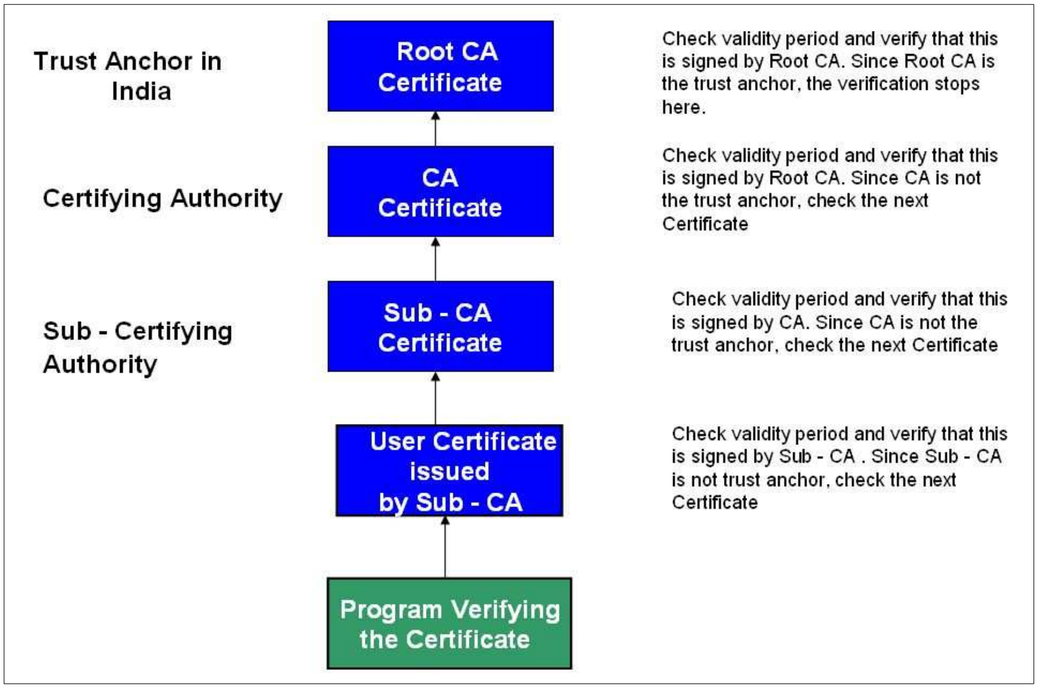

Trust Anchor in India
Root CA Certificate
Check validity period and verify that this is signed by Root CA. Since Root CA is the trust anchor, the verification stops here.
Certifying Authority
CA Certificate
Check validity period and verify that this is signed by Root CA. Since CA is not the trust anchor, check the next Certificate
Sub - Certifying Authority
Sub - CA Certificate
Check validity period and verify that this is signed by CA. Since CA is not the trust anchor, check the next Certificate
User Certificate issued by Sub - CA
Check validity period and verify that this is signed by Sub - CA . Since Sub - CA is not trust anchor, check the next Certificate
Program Verifying the Certificate

Figure: Overview of Root Chain Verification process for Digital Certificates

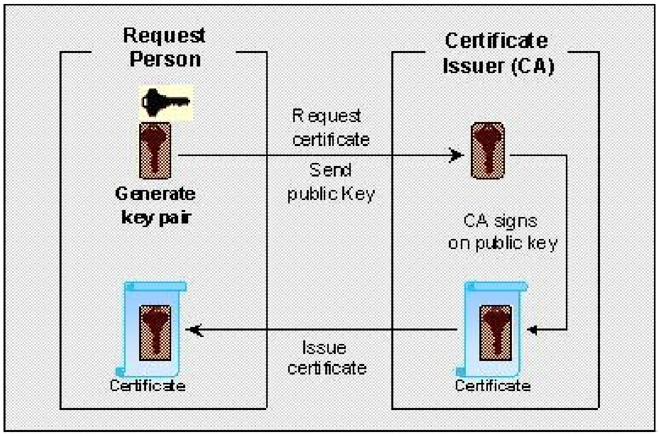
The e-Governance applications should also undertake Root chain verification and CRL verification in addition to the Public Key verification while doing the Digital Signature verification.

19.13 Procurement of Digital Signature Certificates

19.13.1 Overview of the Process

The applicant for the Certificate must generate his/her own key pair and send the public key to the CA with some proof of his/her identity.

The CA will issue a Digital Signature Certificate containing the public key. The CA will digitally sign the certificate using its private key and then send the certificate to the applicant. The CA will check



the applicant's identification before it generates the certificate and signs the request. Different Certifying Authorities may issue certificates with varying levels of identification requirements. One CA may insist on seeing the Identity card while another may want a signed letter authorizing certification from anyone requesting a certificate.

19.13.2 Procedure for procuring Digital Signature Certificates

The CCA has licensed seven Certifying Authorities in India to issue Digital Signature Certificates to the end users. The National Informatics Centre issues Digital Signature Certificates primarily to the Government/ PSU's and Statutory bodies. The Institute for Development of Research in Banking Technology (IDRBT) issues Digital Signature Certificates primarily to the banking and financial sector in India. The remaining five CAs - Safescrypt, TCS, MTNL, n(Code) Solutions and eMudhra issue Digital Signature Certificates to all end users across all domains. More than 16 lakh Digital Signature Certificates have been issued by the different CA's in our country at the time of publication of this document.

(a) Steps for Getting an individual Digital Signature Certificate

1. DSC Form can be downloaded from website of the CA
2. For Class 3 certificate, the applicant has to submit the completed forms in person at the RA
3. On successful processing by the RA, the Username and password are sent to applicant mailbox in order for him/her to log onto CA website. The cryptographic device is handed over to the user for storing the private key.
4. The applicant installs the device drivers for the device (for storing the private key) from CA website.
5. For example:- crypto token, smart card reader
6. User generates the key pair and uploads his Certificate Signing Request (CSR) request into his/her account on the CA Website
7. CA generates the DSC after verification. The user downloads from his/her account on the CA website.

(b) Steps for getting a Web server Digital Signature Certificate

1. Fill in the application form for issuance of an SSL certificate and submit the same to your CA along with applicable fee.
2. Generate a CSR from the Web Server. Kindly note that the tool used for generating the CSR will generate a keystore and save the private key for the CSR on the key store. The key store will have login-id and password which will be required to import the signed public key later. **Note:** The details filled for generation of CSR should be the same as filled in the form submitted to the CA.
3. CA will provide a method to upload / submit the CSR to the CA.
4. On successful processing of the CSR request the CA will generate the SSL Certificate. The same needs to be downloaded from the location specified by the CA in an email.

5. After downloading the SSL Certificate, the Certificate needs to be imported back into the key store using the same tool. Once imported successfully the same is ready for use now.

19.14 Media for Storage of Digital Signature Certificates

It is recommended to store the private key on secure medium, for example, smart cards/ crypto tokens etc. The crypto token connects to the user computer through the USB interface. For smart cards a compatible smartcard reader needs to be installed on the user computer if not already present. The secure media available for the storing the private key may vary per each Certifying Authority.

19.15 Cost

The cost of the Digital Signature Certificate varies from CA to CA. The Certificates are typically issued with one year to two year validity. These are renewable on expiry of the period of initial issue. Further additional fees for renewal may also be charged. The costs involved in procuring Digital Certificates from NIC- CA are attached as a sample. The costs for the other CAs' can be found on their respective websites.

NIC- CA Certificate Fee Structure (For all classes : Class 1, Class 2 and Class 3)

Type of Subscriber	**Smart Card Individual/ Personal Certificate**				**USB Token/iKey Individual/Personal Certificate**			**Soft Token SSL Server / Dev ice Cert. (Proc. Charge)**	**Renewal (Proc. Charges)**
	Smart Card	**Smart Card + Reader**	**Proc. Charge**	**Total**	**USB Token**	**Proc Charge**	**Total**		
Government	227/-	489/-	-	716	555/-	-	555/-		
PSUs & Autonomous / Statutory Bodies	227/-	489/-	200/-	916/-	555/-	200/-	755/-	200/-	200/-
Validity	Two years (Conditions apply)								
Renewal	On expiry of certificate, processing charge shall be applicable as above to renew/create the certificate on the same media. All other formalities shall be same as for a new DSC applicant, including submission of fresh DSC Application form and								

Mode of Payment (Demand Draft/RBI Cheque)

1) **DSC form submitted to NICCA RA Office, Delhi/Chandigarh/Hyderabad:**
DD in favour of "Accounts Officer, NIC Delhi" payable at New Delhi

2) **DSC form submitted to NICCA RA Office, Lucknow:**
DD in favour of "**DDO, NIC UP State Centre**" payable at Lucknow

3) **DSC form submitted to NICCA RA Office, Bangalore:**
DD in favour of "**DDO, NIC Karnataka State Centre**" payable at Bangalore

4) **DSC form submitted to NICCA RA Office, Chennai:**
DD in favour of "**DDO, NIC Tamilnadu State Centre**" payable at Chennai

5**) DSC form submitted to NICCA RA Office, Bhubaneshwar:**
DD in favour of "**DDO, NIC Orissa State Centre**" payable at **Bhubaneshwar**

6) **DSC form submitted to NICCA RA Office, Guwahati:**
DD in favour of "**DDO, NIC Assam State Centre**" payable at **Guwahati**

7) **DSC form submitted to NICCA RA Office, Raipur:**
DD in favour of "**DDO, NIC Chhattisgarh State Centre**" payable at **Raipur**

Also check NIC-CA website (http://nicca.nic.in) for any further updates from time to time.

19.16 Time Taken

The time taken by the Certifying Authorities to issue a DSC may vary from three to ten days.

19.17 Precautions while using Digital Signature Certificates

Digital Signatures are legally admissible in the Court of Law, as provided under the provisions of IT Act 2000. Therefore users should ensure that the Private keys are not disclosed to anyone. For example:- Users generally give their crypto tokes to their personal secretaries or subordinates to sign the documents on their behalf. Any illegal electronic transaction undertaken using a person's private key cannot be repudiated by the certificate owner and will be punishable in the Court of Law.

19.18 e-Governance Applications using Digital Signatures

The following are some of the e-Governance applications already using the Digital Signatures:-

- MCA21 - a Mission Mode project under NeGP which is one of the first few e-Governance projects under NeGP to successfully implement Digital Signatures in their project.
- Income Tax e-filing
- IRCTC
- DGFT
- RBI Applications (SFMS)
- NSDG
- eProcurement
- eOffice
- eDistrict applications of UP, Assam etc

19.19 Usage scenarios for a citizen for Digital Signatures

19.19.1 Context and Overview

A citizen would like to avail various G2C services available at the Common Service Centres(CSC). The following section details the various use case scenarios for a citizen to avail these G2C services.

Please note for the following Use Case scenarios we assume that the digitally signed document that has to be verified is an Income Certificate.

19.19.2 Use Case Scenario for application for a G2C service

In order to avail a G2C service the user would have to undertake the following steps : -

1. The citizen will visit the nearest Common Service Centre.
2. The citizen will put in the application request for the Income Certificate online at the CSC. He will also submit all the necessary documentary proofs at the CSC. This request will be forwarded to the backend Departmental application.
3. The Department will process the request and after successful verification, the authorized Government Officer will issue the Income Certificate by digitally signing it. The same will be stored in the repository of the Departmental application.
4. The citizen revisits the CSC to check the status of the application request. In case the application request has been completed, the CSC operator will be able to show the citizen the Income Certificate from the application repository. In case the Department wishes, they can provide the citizen with a printed copy of the electronic document to furnish for future use.

19.20 Use Case Scenario for Verification of printed copy

In order to avail the various services and benefits, the citizen will have to show the printed copy of the Income Certificates to various Departments. In order to verify the printed copy of the Income Certificate, the verifier (Department Officer to whom the citizen furnishes the document for availing a service) has the following three options

1) Via Request ID

1. The verifier can go to the Department website and search by the Unique Request ID printed on the Income Certificate.
2. The electronic version of the Income Certificate will be displayed on the website to the verifier.
3. The verifier can compare fields of the Income Certificate displayed in the website with the hardcopy presented by the citizen and thereby verify the authenticity of the document.

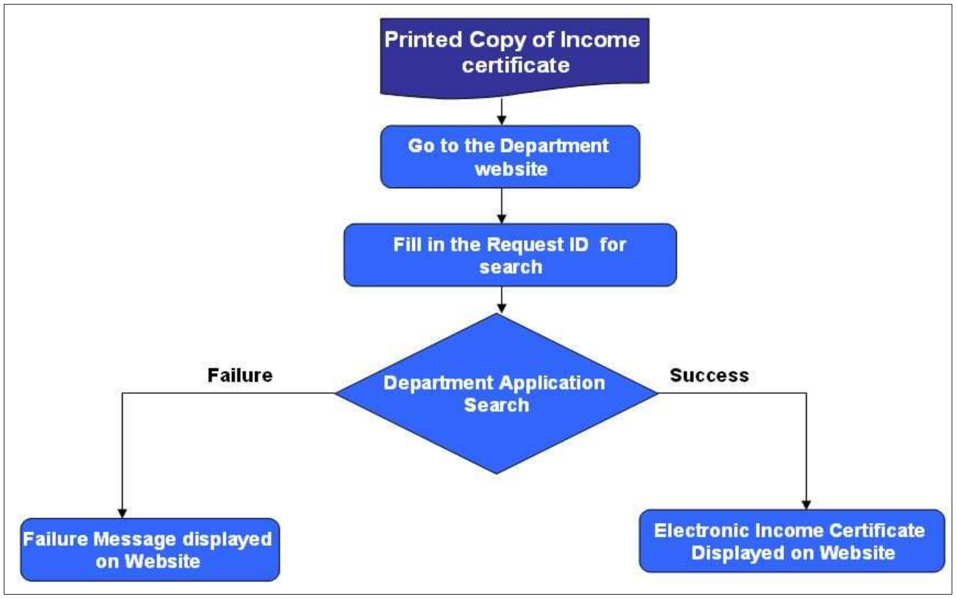

Printed Copy of Income certificate
Go to the Department website
Fill in the Request ID for search
Department Application Search
Failure
Success
Failure Message displayed on Website
Electronic Income Certificate Displayed on Website

Figure: Verification of Income Certificate by Request ID

2) Via 2D Barcode

The Income Certificate can have a 2D barcode in which the digital signature is embedded. In case a 2D barcode is present on the Income Certificate, the verifier has the following two options to verify the printed copy of the Income Certificate

2.1 Online Verification

The verifier will be required to have an Internet Connection and a 2D barcode reader for this option.

1. The citizen will scan the 2D barcode from the printed copy of the Income Certificate
2. The output from the scanner will be fed to the verification utility of the Department (can be downloaded from the Department website)
3. The verification utility of the departmental application will verify the digital signature embedded in the barcode with the one stored in the database.
4. In case the signatures match, the verification utility will display the electronic version of the Income Certificate on the Department website.
5. The verifier can verify the contents of the Income Certificate with that of the Income Certificate displayed on the website.

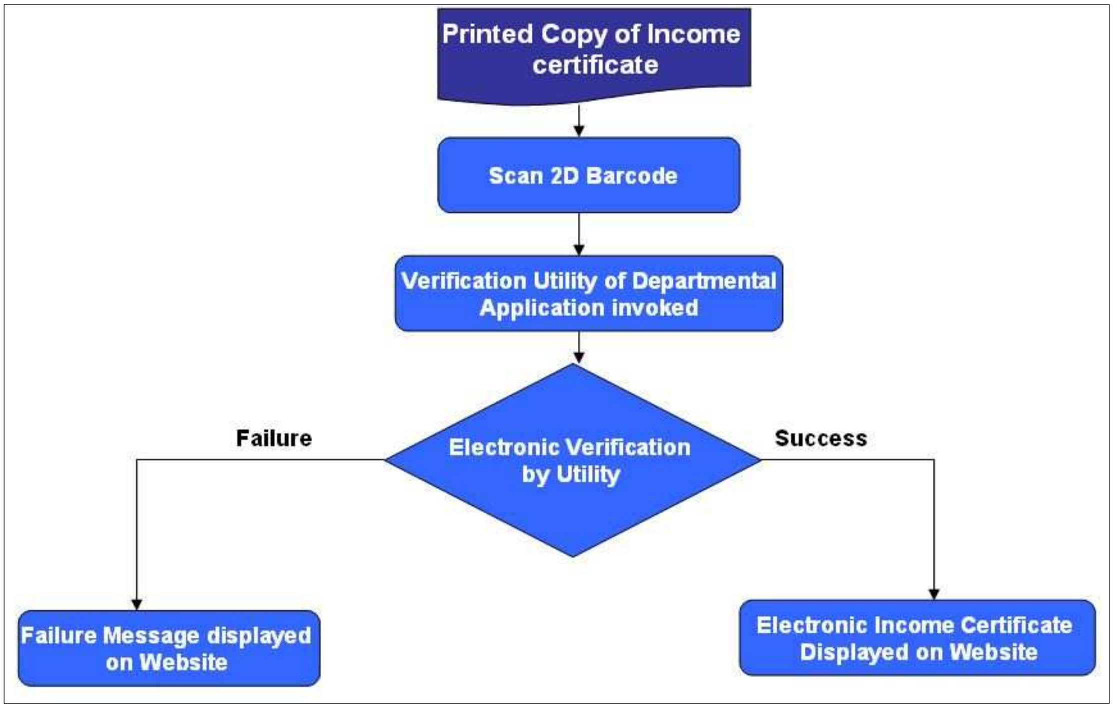

Printed Copy of Income certificate
Scan 2D Barcode
Verification Utility of Departmental Application invoked
Electronic Verification by Utility
Failure
Success
Failure Message displayed on Website
Electronic Income Certificate Displayed on Website

Figure: Online Verification of Income Certificate by citizen

2.2 Offline Verification

The citizen will be required to have a Computer, a 2D barcode reader, Public Key of the Taluka official who signed the Income Certificate, Root Chain Certificate of the CCA and NIC-CA and the verification utility of the departmental application. No connection to internet will be required.

In case the verifier does not have the above softwares installed on the computer, he can follow the underlying steps to install the softwares, This is a one time activity.

1. The verifier will download the root chain certificates of CCA from the CCA website (http://cca.gov.in/rw/pages/rcai_root_certificate.en.do) and NIC-CA certificate from the NIC-CA website (http://nicca.nic.in/index.jsp).
2. The public key of the taluka official can be downloaded from the NIC-CA website by searching for the name of the Taluka official on the website.
3. The verifier will install the verification utility of the departmental application by downloading it from the respective department website.

The verifier will have to undertake the following steps to verify the printed copy of the Income Certificate:

1. The verifier will open the verification utility.
2. The verifier will use a barcode reader to scan the 2D barcode from the printed copy of the Income Certificate.
3. The verification utility will verify the digital signature scanned from the document.
4. The verification utility will accordingly display the appropriate message to the verifer.

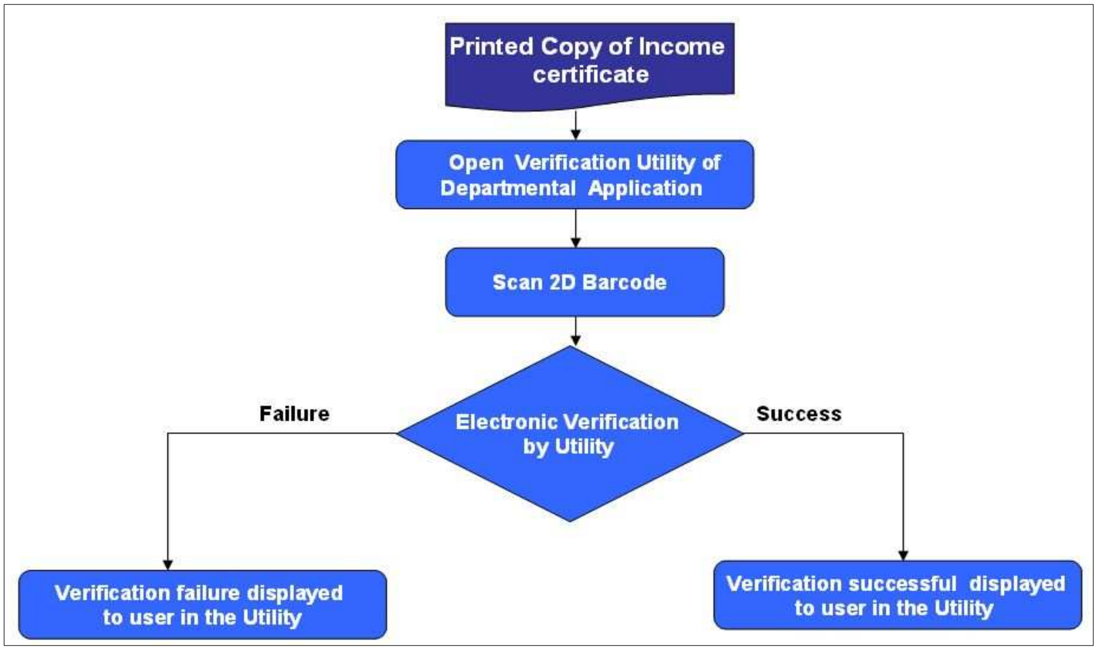

Printed Copy of Income certificate
Open Verification Utility of Departmental Application
Scan 2D Barcode
Electronic Verification by Utility
Failure
Success
Verification failure displayed to user in the Utility
Verification successful displayed to user in the Utility

Figure: Offline Verification of Income Certificate by citizen

19.21 Frequently Asked Questions about Digital Signatures

Q.1: What is Cryptography?

Cryptography is the science of enabling secure communications between a sender and one or more recipients. This is achieved by the sender scrambling a message (with a computer program and a secret key) and leaving the recipient to unscramble the message (with the same computer program and a key, which may or may not be the same as the sender's key).

There are two types of cryptography: Secret/Symmetric Key Cryptography and Public Key Cryptography.

Secret key (symmetric/conventional) cryptography - is a system based on the sender and receiver of a message knowing and using the same secret key to encrypt and decrypt their messages. One weakness of this system is that the sender and receiver must trust some communications channel to transmit the secret key to prevent from disclosure. This form of cryptography ensures data integrity, data authentication and confidentiality.

Public key (asymmetric) cryptography - is a system based on pairs of keys called public key and private key. The public key is published to everyone while the private key is kept secret with the owner. The need for a sender and a receiver to share a secret key and trust some communications channel is eliminated. This concept was introduced in 1976 by Whitfield Diffie and Martin Hellman.

The Digital Signatures created using the private key ensure data integrity, data authentication and non- repudiation. However, to ensure confidentiality, encryption of the data has to be done with the recipient's public key.

Q.2: How do I get a Digital Signature Certificate?

The Office of Controller of Certifying Authorities (CCA), issues Certificate only to Certifying Authorities. The CAs in turn issue Digital Signature Certificates to the end-users. You can approach any of the CAs for getting the Digital Signature Certificate. For more information about the respective CAs, visit their websites indicated below:-

Name of CA	Website
Safescrypt	www.safescrypt.com
National Informatics Centre	www.nic.in
Institute for Development and Research in Banking Technology (IDRBT)	www.idrbtca.org.in
TCS CA services	www.tcs-ca.tcs.co.in
MTNL CA services	www.mtnltrustline.com
(n) Code Solutions	www.ncodesolutions.com
eMudhra	www.e-Mudhra.com

Q.3: What is a Certifying Authority (CA)?
A CA is a trusted third party willing to verify the ID of entities and their association with a given key, and later issue certificates attesting to that identity. In the passport analogy, the CA is similar to the Ministry of External Affairs, which verifies your identification, creates a recognized and trusted document which certifies who you are, and issues the document to you.

Q.4: Who are the CAs licensed by the CCA?

1. Safescrypt b. NIC
2. IDRBT
3. TCS
4. MtnlTrustline f. GNFC
5. e-MudhraCA

Q.5: If CA is out of business then if the subscriber is told to move to another CA then the subscriber has to get a new digital certificate. What happens to his/her earlier transactions? Does this not create a legal and financial problem?

Prior to cessation of operations the CA has to follow procedures as laid down under the IT Act. Such problems should not therefore exist.

Q.6: Can one authorize someone to use DSC?
Incase a person wants to authorize someone else to sign on his/her behalf, than the person being authorized should use their own PKI credentials to sign the respective documents.

Q.7: Can a person have two digital signatures say one for official use and other one for personal use?
Yes.

Q.8: In paper world, date and the place where the paper has been signed is recorded and court proceedings are followed on that basis. What mechanism is being followed for dispute settlements in the case of digital signatures?
Under the IT Act, 2000 Digital Signatures are at par with hand written signatures. Therefore, similar court proceedings will be followed.

Q.9: Is there a "Specimen Digital Signature" like Paper Signature?
No. The Digital signature changes with content of the message.

Q.10: If somebody uses others computer, instead of his own computer, then is there any possibility of threat to the security of the owners/users digital signature?

No, there is no threat to the security of the owner / users digital signature, if the private key lies on the smartcard /crypto token and does not leave the SmartCard/crypto token.

Q.11: Is it possible for someone to use your Digital Signature without your knowledge?

It depends upon the how the signer has kept his private key. If private key is not stored securely, then it can be misused without the knowledge of the owner. As per the IT Act 2000, the owner of the private key will be held responsible in the Court of Law for any electronic transactions undertaken using his/her PKI credentials(public/private keys).

Q.12: When you cancel an earlier communication you can get it back, how does this work in e-environment?

A new message saying that the current message supersedes the earlier one can be sent to the recipient(s). This assumes that all messages are time stamped.

Q.13: When can a DSC be revoked?

The DSC can be revoked when an officer is transferred, suspended or his/her key is compromised.

Q.14: How do digital certificates work in e-mail correspondence?

Suppose Sender wants to send a signed data/message to the recipient. He creates a message digest (which serves as a "digital fingerprint") by using a hash function on the message. Sender then encrypts the data/message digest with his own private key. This encrypted message digest is called a Digital Signature and is attached to sender's original message, resulting in a signed data/message. The sender sends his signed data/message to the recipient.

When the recipient receives the signed data/message, he detaches sender's digital signature from the data/message and decrypts the signature with the sender's public key, thus revealing the message digest.

The data/message part will have to be re-hashed by the recipient to get the message digest. The recipient then compares this result to the message digest he receives from the sender. If they are exactly equal, the recipient can be confident that the message has come from the sender and has not changed since he signed it. If the message digests are not equal, the message may not have come from the sender of the data/message, or was altered by someone, or was accidentally corrupted after it was signed.

Q.15: How do Digital Certificates work in a web site?

When a Certificate is installed in a web server, it allows users to check the server's authenticity (server authentication), ensures that the server is operated by an organization with the right to use the name associated with the server's digital certificate. This safeguard's the users from trusting unauthorized sites.

A secure web server can control access and check the identity of a client by referring to the client certificate
(client authentication), this eliminates the use of password dialogs that restrict access to particular users.

The phenomenon that allows the identities of both the server and client to be authenticated through exchange and verification of their digital certificate is called mutual server-client authentication. The technology to ensure mutual server-client authentication is Secure Sockets Layer (SSL) encryption scheme.

Q.16: What clause an e-Governance project should have to ensure that the PKI implementation meets the requirement of the IT Act 2000?

The e-Governance applications have to be developed in compliance with RFC5280 certificate profile. A number of commercial and open source PKI toolkits are available which can be used to develop a standard validation process. Eg : - Microsoft CNG, Sun Java Toolkit.

Q.17: Can I use the certificate issued by a CA across e-Governance applications ?
Yes.

Q.18: What are the key sizes in India?
CA Key is 2048 bits and the end user keys are 1024 bits. However from 1 Jan 2011, the end user keys will be
2048 bits as well as per the notification by CCA.

Q.19: What is the size of digital signatures?
The size of the Digital Signatures varies with the size of the keys used for generation of the message digest or hash. It can be a few bytes.

Q.20: What is the Key Escrow?
Key escrow (also known as a fair cryptosystem) is an arrangement in which the keys needed to decrypt encrypted data are held in escrow so that, under certain circumstances, an authorized third party may gain access to those keys. These third parties may include businesses, who may want access to employees' private communications, or governments, who may wish to be able to view the contents of encrypted communications.

Q.21: What are the documents accepted by NIC - CA for verification?
Any of the following IDs are accepted by NIC-CA for verification of CSR:

1. Employee ID
2. Passport Number
3. Pan Card Number
4. Driving License Number
5. PF Number
6. Bank Account Details
7. Ration Card No

Q.22: How do applications use the CRLs?
The applications download the CRLs from the respective CA sites at a specified frequency. The applications than verify the public keys against this CRL at the time of Digital Signature verification. The CCA is in the process of implementation of the OCVS (Online Certificate Verification Service) . This will ensure online verifications of the CRLs by the applications.

Q.23: How long do the CAs' in India preserve the Public Keys of the end users?
As per the IT Act 2000, each CA is stores the Public Key in their repository for a period of 7 years from the date of expiration of the Certificate.

Q.24: Should e-Governance applications archive the Digital Signature Certificates as well?
In view of the fact that the CAs have a mandate to save the DSCs for a period of 7 years, it may be advisable for the e-Governance applications which would need to verify the records for authenticity for periods beyond 7 years.

Q.25: Can I have multiple Digital Signatures to a document?
Yes one can have multiple Digital Signatures to a document. For eg: - in the MCA21 application the forms are signed by different Directors as part of the application workflow.

Q.26: What are the types of applications that should use Digital Signatures?
The e-Governance applications mainly provide:

1. Information Services
2. Interactive Services (downloading of forms etc)
3. Transaction Services with or without payments like issuance of various Certificates etc

The category 3 services (transaction based) can benefit from the use of digital signatures. In general wherever a e-Governance application requires handwritten signatures during the workflow of a document in the approval process, we should replace them with Digital Signatures.

Q.27: What are cryptotokens?
They are hardware security tokens used to store cryptographic keys and certificates. Eg :- USB etc

Q.28: What are the different ways of authenticating content of digitally signed documents issued to the citizen?
There are different ways of verifying the content and the digital signatures of the document. Some of the mechanism are enlisted below:-

1. Via Unique Request 10 (manual content verification only) · In this process the user can verify the validity of his/her document by logging onto the Department website and providing the unique request number printed on the document. The Department application will display the electronic version of the document stored in the application repository. However in this process since the digital signature on the document is not verified, the contents have to be verified manually by the user by comparing the online document from the website with the hardcopy of the document. This process thus provides content verification only. The verification of the Digital Signature does not take place in this process.

2. Verification by the 20 Barcode - In this process, the barcode printed at the bottom of the document is used for the digital signature verification. The barcode has the Digital Signature embedded in it. The two verification mechanisms enlisted below verify the Digital Signature only. Since the complete content of the document is not being scanned, the content verification has to be done manually.

a) Online Verification
In this process, a barcode reader is used to scan the 2-D bar code printed at the bottom of the certificate. The verification utility of the Departmental application would verify the digital signature embedded in the document and after successful verification, show the corresponding electronic record on their website. However the user needs to compare the contents of the electronic record and the hardcopy. This method requires a computer, an internet connection and a 2D bar code reader.

b) Offline Verification
In this process, the user can verify the digital signature embedded in the barcode without connecting to the Department website. Thereby this process is called as "offline" verification. The user needs to download and install the verification utility custom developed by the Department (downloadable from their website). The user also needs to download the root chain certificates of CCA and NIC and the public key of the authorised taluka and the taluka official onto the computer. Once these items are installed on the computer, the user can scan the 2D barcode on the document and the verification utility will check the validity of the digital signature embedded in the document thereby proving the authenticity of the document. However, the content of the hardcopy of the document will have to be manually verified by the comparing with the electronic version available at the Department website as the content of the hardcopy is not being scanned in this process.

Q.29: How can a digitally signed document be verified after the 0SC associated with the Public Key has expired?
The digital signature verification process for a document requires the public key, root chains and the CRL. The e-Governance application should therefore have a repository of public key certificates, root chains and the CRL's of the time the document was digitally signed. The CA's as of now are mandated to store the Digital Signature

Certificates, root chains and the CRLs for a period of 7 years as per the Rules of the IT Act. Therefore the Digital Signature Certificates can be downloaded from the CAs for a period of 7 years. However, if the digital signature on the document needs to be verified after this period, the e-Governance applications will have to have a provision to store the DSCs, root chains and the CRLs in a repository and undertaking the verification of digitally signed document against this repository. However, it may be a cumbersome process to get the CRLs' from the respective CAs for a specific period (in the past).

Q.30: How can Departments ensure that their Government officers authorized to sign the Certificates do not misuse their Digital Signature Certificates after being transferred from a given place?

It is recommended that as part of the handing over of charge of a given officer, the DSC issued to the officer be revoked. Further his user credentials in the respective e-Governance applications should be deactivated so that he can no longer access the application while the Certificate revocation is under process with the CA. Once the DSC is successfully revoked, the officer will be no longer able to sign the documents.

Q.31: How can a citizen be assured that the document has been digitally signed by the appropriate authorized Government officer?

In order to ensure that the documents are signed by authorized individuals only, the Departments should maintain a repository having a mapping between the DSC and the respective roles assigned to the officers of the Departments. The e-Governance application should check against this repository for the various documents before allowing an officer to digitally sign the document. This mechanism has been implemented in MCA21 application wherein multiple directors sign the eforms for the application. The key challenge with this approach is to be able to maintain an updated repository at all times.

The Government of India is currently looking into the proposal for creation of a central repository of Digital Signature Certificates and CRLs' in order to ensure that digitally signed documents can be verified at a later date (greater than 7 years).

20. Critical issues in e-Governance

20.1 Introduction

We have seen that e-Governance is an online helping hand from the Government to the people and vice versa. Proper use of e-Governance is helpful to run the democracy smoothly. But it has many issues and challenges which are to be faced by the Government and the people as well. Let us have a look on these issues and challenges, and discuss some remedies to overcome these issues.

20.2 Issues in e-Governance

20.2.1 Technical Issues

1. **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.

2. **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.

3. **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.

4. **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.

20.2.2 Economic Issues

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

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

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

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

20.2.3 Social issues

1. **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.

2. **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.

3. 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.

4. 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.

5. Awareness in rural areas: in India, 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.

20.3 Implementation aspects of e-Governance

The implementation of e-Governance system has many aspects. For example, 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 aptly indicates various implementation aspects of e-governance. This 7-Cs are as under:

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 valid as a legal documents.

20.4 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.

20.5 Reasons for failures

e-Governance projects may fail due to multiple reasons. The reasons usually listed are neither comprehensive nor complete. Some of these reasons are as under:

1. Planning to fail or Failing to plan: The first step in any project is planning. The success of the project will depend on the skill and expertise with which it is planned and conceptualized. The plans are finalized without clear objectives, unclear roles and responsibilities. There are no parameters for financial controls. Areas like risk assessment, feasibility assessment, prioritization and strategy are not even thought about. So where as no plans exists in some projects, in others, the plan is doomed for failure.

2. Mission Impossible: Another cause of project failure is to visualize the impossible. The project consultants hired by various government departments generally promise the moon to the dep. They expect that whatever they suggest will be implemented by the government without realizing the fact that the government has its own limitations. The reality and the vision gap is the second step towards e-governance failure.

3. Misunderstanding governance: The consultant hired by the government at times totally misunderstands the governance process and the institution of the government. They do not realize that the government will be governed by the constitution and the laws therein. Consultants feel that the government will change according to the solution suggested by them. They have an impression that the government has to fit into their solution and not vice versa. In reality they have no ensure that their solutions fit the government needs. Further the consultants do not realize that the government is the complex structure which has existed over the years and any big changes are very difficult to implement. Misunderstanding the government and governance is the third step leading to the failure of e-governance projects.

4. **Bottleneck is at the top of the bottle always: T**he various departments in the government of India are mostly headed by individuals who are nearing their retirement. The top officials are lovers of status quo and develop resistance to change. With no support from top leadership, the e-governance projects do not get any encouragement.

5. **Focus on 'e' rather than 'governance':** Every seminar, every author, every government officer stresses that e-governance is more about governance than 'e'. However the implementers in the government have not realized the importance of the same. The team for this program management unit must comprise individuals with experience in diverse government background. Focus on IT and electronics is the another most important cause of failure of e- governance.

6. **Employees as stakeholder universe:** Majority of the projects take government employees as the only stakeholders. The consultation process happens with the senior government employees and rest of the stakeholders are neglected. The government departments feel that they know all the requirements of the stakeholders and therefore it is useless spending time on such projects. The stakeholder universe being limited to employees, is another cause of failure.

7. **Let's build Rome in a day:** Most of the e-governance projects are given unachievable timelines. Most of the time ministers or leaders make announcements and the deadlines, then the quality becomes the key challenge in project implementation. It may take time for an e-governance project to actually be ready to be launched and it may take time for training and adoption of the project by all stakeholders. A change is not easy to implement and we must be patient in implementing change via e-governance. The time taken will further help to improve and rectify the project. Unachievable timeless and the race to achieve them is a further cause of failure.

8. **Individual projects:** Most of the e-governance projects are individual-driven. The approach of individualizing the project is not appropriate and this leads to failure. The project which are driven by individuals die after the individuals leave the organizations. But project which have been institutionalized stay forever.

9. **Procedural loops:** The procedural loops are another hindrance in the e-governance project implementation. All projects need to go through a competitive bidding process which may take even more than the implementation of the project. Sometimes even, the project approval time is more than the implementation time. The project files keep on moving from one department to another and from one table to another. This causes to failure.

10. **From office vs. back office e-governance:** Unless the backend integration of systems take place, the frontend efforts may not lead to any success. The true e-governance applications will be achieved only when the front office is integrated with the backend application. Creating front offices without any back office integration is another cause of e- governance failure.

20.6 e-Governance Action Plan

Government of India is now beginning to realize that e-governance is the key to drive today's economy with an increased participation from citizens. Providing services online is no longer going to remain optional for local and central government, as demand for providing services at internet speed has been coming from citizens. The real challenge is how to develop and sustain successful e-Governance projects and deliver state of the art e-services to citizens. Some of the requirements for implementing successful e-governance across the nation are as under.

1) E-governance framework across the nation enough bandwidth to service a population of one billion.

2) Connectivity framework for making the services reaches rural areas of the country or development of alternative means of services such as e-governance kiosks in regional language.

3) National citizens database which is a the primary unit of data for all governance vertical and horizontal applications across the state and central governments.

4) e-Governance and interoperability standards for the exchange of secure information with non- repudiation across the state and the central government seamlessly.

5) A secure delivery framework by means of virtual private network connecting across the state and the central government departments.

6) Data centers in the state and the central government to handle the departmental workflow automation, collaboration, interaction, exchange of information with automation.

20.7 Some recommendations for success

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.

a) 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.

b) 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 e-awareness exercise should be carried out in all state government departments, to understand their level of acceptability of the e-governance.

c) 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.

d) 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.

e) 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.

f) 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.

g) 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.

20.8 Summary

Though, government is trying to give its best services to the people, there are many problems like illiteracy, large population, poverty etc. e-Governance helps the government to avoid these problems and reach to the people. But it has also some issues and challenges. With the proper use of e - governance these problems can be solved and people can get better services from the government.

21. Why e-Governance projects fail

21.1 Introduction

We have seen that e-Governance is looked upon as a means to change the very concept of governance resulting in empowerment of citizens and increased transparency in public dealings by governments, and increased efficiency in delivery of public goods is an inherent underlying assumption. This chapter shares some of the problems that may derail the process and need to be guarded against by vigilant auditors who should bring these to public attention in a timely fashion.

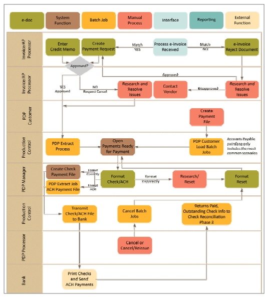
The concept “e-Governance” may sound quite attractive to our millions of fellow citizens. However according to an oft quoted 2003 survey on e-Government initiatives in developing or transitional countries, only 15 per cent of e-Government projects can be termed as successful, with 35 percent as total failures and 55 percent as partial failures where the outcome is classified as follows:

- Total failure: the initiative was never implemented, or was implemented but immediately abandoned.
- Partial failure: major goals for the initiative were not attained and / or there were significant undesirable outcomes.
- Success: most stakeholder groups attained their major goals and did not experience significant undesirable outcomes.

Though this survey was on ‘e-Government’ and not ‘e-Governance’, a very large number of e-Governance projects have, over the years, belied the promise that they once showed.

The Government, over the last few years, has conducted numerous audits of e-Governance projects with the scope ranging from evaluating the system development methodology to the overall performance in terms of the achievement of objectives. The results brought into focus the fact that the issue of e-Governance is much more than a technological initiative but is made of a complex set of relationships between the stakeholders’ commitment, structured developmental processes and adequate infrastructural resources. There were a number of reasons for e-Governance projects not doing well or falling short of expectations. Many should be applicable across national boundaries and could serve as guiding points for the auditors. Some of the more important ones are discussed below:

Reason 1: Lack of business process modification



In many well meaning projects, duplication of the manual processes in the IT environment were seen as major reasons for the end users / citizens not associating any value addition with the projects and looked upon e-Governance as an unwelcome addition to the hurdles to be crossed before getting 'the work done'. For example, in departments which maintain land records especially in rural areas the details regarding land ownership, cropping patterns etc. were computerized but no legal sanctity was given to the output generated by such systems in absence of a commensurate change in the statutes. Similarly, lack of horizontal integration also means that e-Governance projects would continue to deliver services in a fragmented and unsatisfactory fashion resulting in the end users having to approach a multitude of Government agencies thus defeating the promise of 'less government in your life'.

Moreover an ambiguity about the very concept of e-Governance results in many government entities categorizing e-Government projects such as office automation and inventory management as e-Governance projects. Thus, vast amounts of money are spent on computerization activities without giving the benefits of e-Governance to the end users.

Reason 2: Vendor-driven initiatives

Currently, e-Governance is the buzzword in the corridors of power in Governments and the international donor agencies. Large funds are being promised and given to implement such schemes.

However a close scrutiny startlingly reveals, that the preference for IT components such as the hardware and software such as operating systems and RDBMS change dramatically for similar projects within the same country in the same period of time. While there may be only limited objections to choosing one technology over the other, auditors need to monitor and examine the trends.

It is also seen that often the acquisition and implementation processes are not monitored in an effective fashion and deliverables are often less than the specifications. However, due to a hurry to 'get things going' quickly, the projects may be commissioned or launched even when they are not fully ready. Moreover, it is not only in the acquisition and implementation but also in the delivery and support areas that excessive dependence on the developers / vendors is seen resulting in large revenue expenditure while the untrained work force of the Government entities sits idle. Additionally, there is often poor control over outsourcing. The benchmarks for evaluating performance of the service provider are not set out in a transparent fashion and are often biased towards it. For example, a penalty clause for deficient services and extended liability is often absent or too poorly drafted to be legally enforceable.

This completes the chain which started from lack of transparency in selection of technology / vendor, passed through less than adequate receipt of deliverables, and went through to large payments for services which are not monitored for performance. Ultimately, the citizen or the governed is the only loser.

Reason 3: Individual led initiatives

In many projects at the system development stages, especially when the user requirements were being made, there is lack of effective communication between the users to share the domain knowledge with the system developers. This is particularly true of projects which were being implemented as a result of individual initiatives emanating from the top of the management hierarchy. In such cases, the developers also felt answerable to none except the management at the very top. This soon caused even the enthusiasts at the operational level to lose interest and the projects are implemented by 'going though the motions'. This led to the development of systems which were inherently deficient, and which soon ran into the ground after the change of guard at the top management level. Even where the systems become operational and are hailed as success stories, poor change management controls mean that over a period of time they completely stop doing what they had set out to achieve.

Sometimes e-Governance projects, paradoxically, become victims of their own success. The demand for the services rendered by them may end up outstripping the capacity both of the infrastructure and of the organizational preparedness. This is especially true in cases of 'start small, rollout fast and scale big later' model which is increasingly gaining popularity.

Reason 4: Vested interests

It is often seen that there was clearly stated commitment from the Political establishment but continuous resistance by a section of the executive and other stakeholders adversely affected by transparency brought in by e governance.

“e-Governance” is a catchy slogan which translates into 'power to the people', and paints a picture where the omnipotent computers would take over all those functions of the Government which entail an 'unnecessary' interaction of the common man with a Government official. This immediately attracts the fancy of the citizens who are also potential voters, and look forward to a corruption-free and discretion-free system where each individual is treated according to transparent rules. This enthusiasm for IT enabled e-Governance allows the governments to announce and launch mega e-Governance schemes which often translate into large scale expenditure on hardware and software. These are often associated with lack of transparency in acquisition and creation of technological and physical infrastructure, an irony since the projects themselves seek to increase transparency in the governance mechanisms.

However, there may also be lobbies which feel threatened by this transparent governance and often they may be seen to do anything to either discredit a new project, or to not allow it to take off at all. Though the fear of unemployment resulting from computerization is long dead, the resistance continues as it has been realized that automation of backend procedures would eventually result in e-Governance.

Reason 5: Confidentiality issues

A major concern is the lack of attention to issues relating to the confidentiality of the data, such as in e-Tendering systems or regarding personal details of citizens etc.

For example, if an e-Tendering system does not store the data regarding the bids before the opening date in unencrypted fashion, PKI is not mandatory for submission of bids, logical time locks to disable access to the bid details before the bid opening date are absent and there is inadequate provision of activity logs for system and data administrator activities then the system can be labelled as extremely prone to manipulation and does more harm to the cause of IT in improving governance.

One may be surprised to find such cases where large contracts have been decided on the basis of such a system. Information Technology is, indeed, a two-edged weapon!

Similarly, if personal details such as social security numbers or taxation details in an e-Tax Return Filing System are not kept in a secure environment, it would ultimately undermine the confidence of the users in the use of such systems.

Ironically, IT-enabled e-Governance can also facilitate frauds. It was observed that in cases of computerized 'lucky draws' for houses / residential plots the algorithm was tampered with to favour a few. This was completely contrary to the spirit of a 'lucky' draw where the results should be random. As a result, some sections of citizens started blaming IT for the problem. Clearly the issue was not one of IT enabled fraud but of the organization not addressing the risk arising from the very nature of technology.

Reason 6: The digital divide

There is always a risk that the implementation of e-Governance projects is prioritized so as to benefit only a certain section or sections of the society. Additionally, e-Governance delivery mechanisms may not account for the existing digital divide. This would cause even the most well intentioned initiatives to not achieve their objectives. Though innovative methods were seen, especially such as e-Governance kiosks manned by paid non- government facilitators to help citizens, the fact remains that without bridging the digital divide e-Governance projects may not gain critical mass to be effective.

Successful e-Governance implementation is about four main components. End users need:

- Identification;
- Business Process Modification;
- Use of Information Technology; and most importantly
- Committed Government Intent

Deficiencies in any of these would result in e-Governance projects failing to achieve their objectives.

21.2 A word of caution

Identifiable and measurable parameters to assess the success of e-Governance projects are not easy to formulate. This is especially true regarding the intangible / soft benefits which are in the forms of increased transparency, sense of economic and social empowerment by access to information and better efficiencies in delivery of public services. In the absence of benchmarking, due to the uniqueness of some of the projects, making a quick judgment about their success or failure is a risk that must be guarded against by all auditors and assessors.

22. Relevant websites and further reading resources

1. **e-Governance Initiatives in India**
   http://arc.gov.in/11threp/ARC_11thReport_Ch4.pdf
2. **Maharashtra e-Governance Policy**
   http://it.maharashtra.gov.in/1083/Maharashtra-eGovernance-Policy
3. **NeGP**
   https://www.negp.gov.in/
4. **Governance Knowledge Centre**
   http://www.indiagovernance.gov.in/
5. **Department of Electronics & Information Technology (DeITY), GoI**
   http://deity.gov.in/
6. **National Institute of Smart Government**
   http://www.nisg.org
7. **Second Administrative Reforms Commission Report**
   http://arc.gov.in/11threp/ARC_11th_report.htm
8. **India Development Gateway**
   http://www.indg.in/
9. **India Portal**
   http://www.india.gov.in
10. **Informatics (NIC)**
    http://informatics.nic.in/
11. **Saaransh – A Compendium of MMPs**
    http://deity.gov.in/sites/upload_files/dit/files/Compendium_FINAL_Version_220211.pdf
12. **United Nations Public Administration Network (UNPAN)**
    http://www.unpan.org
13. **National e-Governance Service Delivery Gateway**
    http://www.nsdg.gov.in
14. **World Bank Group**
    http://www.worldbank.org
15. **e-Governance Standards**
    http://egovstandards.gov.in
16. **Major e-Governance Projects**
    http://www.egovindia.org/egovportals.html
17. **Common Service Centers Scheme**
    http://csc.gov.in/
18. **Department of Administrative Reforms and Public Grievances, GoI**
    http://darpg.gov.in/
19. **e-Governance in India (private Blog)**
    http://egovindia.wordpress.com/

Annexure I

Glossary

Abuse of privilege

Formal nomenclature for user action not in accordance with organizational policy or law. Actions falling outside, or explicitly proscribed by, acceptable use policy.

Accountability

The principle that individuals using a facility or a computer system must be identifiable. With accountability, violations or attempted violations of system security can be traced to individuals who can then be held responsible.

Acceptable level of risk

A judicious and carefully considered assessment by the appropriate authority that a computing activity or network meets the minimum requirements of applicable security directives. The assessment should take into account the value of assets, threats and vulnerabilities, counter-measures, and operational requirements.

Active attack

A form of attack in which data is actually modified, corrupted, or destroyed.

Adapter

A device that serves as an interface between the system unit and a device attached to it, such as a SCSI Adapter. Often synonymous with expansion card or board. Can also refer to a special type of connector.

Advanced WWW Counter

Full-featured advanced counter that is highly customizable, allowing you to change digit formats, colors, time, and adjustable data counts.

Ambient data

This is a forensic term that describes, in general terms, data stored in non-traditional computer storage areas and formats. The term was coined in 1996 to help students understand computer evidence-processing techniques that deal with evidence not stored in standard computer files, formats, and storage areas. The term is now widely used in the computer forensics community and it generally describes data stored in the Windows swap file, unallocated space, and file slack.

Anomaly detection

A label for the class of intrusion detection tactics that seek to identify potential intrusion attempts by virtue of their being (presumably) sufficiently deviant (anomalous) in comparison with expected or authorized activities. Phrased another way, anomaly detection begins with a positive model of expected system operations and flags potential intrusions on the basis of their deviation (as particular events or actions) from this presumed norm.

Antivirus

Software that detects, repairs, cleans, or removes virus-infected files from a computer.

Application

A more technical term for program.

Application gateway

One form of a firewall in which valid application-level data must be checked or confirmed before allowing a connection. In the case of an ftp connection, the application gateway appears as an ftp server to the client and an ftp client to the server.

Assurance

A measure of confidence that the security features and architecture of an information system or network accurately reflect and enforce the given security policy.

Asynchronous attacks

Attacks that take advantage of dynamic system actions-especially by exploiting an ability to manipulate the timing of those actions.

Attitudes

Positively or negatively learned orientations toward something or someone that have a tendency to motivate an individual or group toward some behavior. Experienced soldiers, for example, have negative attitudes toward slovenliness.

Audit trail

In computer security systems, a chronological record of when users login, how long they are engaged in various activities, what they were doing, and whether any actual or attempted security violations occurred. An automated or manual set of chronological records of system activities that may enable the reconstruction and examination of a sequence of events or changes in an event.

Auto responders

Sends an automated email response to incoming mail sent to a specific address. For instance, you can have your visitors send an email to info@ yourdomain.com to get an email explaining your latest product or automatically reply to orders with a prewritten thank you email message.

Back door

A hole in the security of a computer system deliberately left in place by designers or maintainers. Synonymous with trap door. A hidden software or hardware mechanism used to circumvent security controls. A breach created intentionally for the purpose of collecting, altering, or destroying data.

Bandwidth

Bandwidth is the sum of all the data transferred from and to your Web site, including email, Web pages, and images. See "Monthly Traffic."

Bank

The collection of memory chips or modules that make up a block of memory. This can be one, two, or four chips. Memory in a PC must always be added or removed in full-bank increments.

Between-the-lines entry

Access that an unauthorized user gets, typically by tapping the terminal of a legitimate user that is inactive at the time.

BIOS

The part of the operating system that provides the lowest level interface to peripheral devices. The BIOS is stored in the ROM on the computer's motherboard.

BLOB

Binary large object used to describe any random large block of bits, usually a picture or sound file; can be stored in a database but is normally not interpretable by a database program. Can be used as a mild hacker threat (mailbomb) when mailed. Can also be used to hide malicious logic code.

Blue box devices

Gadgets created by crackers and phone hackers ("phreakers") to break into the telephone system and make calls bypassing normal controls and billing procedures.

Boot

To start up your computer. Because the computer gets itself up and going from an inert state, it could be said to lift itself up "by its own boot straps"-this is where the term boot originates.

Boot Record

Once the BIOS determines which disk to boot from, it loads the first sector of that disk into memory and executes it. Besides this loader program, the boot record contains the partition table for that disk. If the boot record is damaged, it can be a very serious situation.

Bootstrap

To load and initialize the operating system on a computer. Often abbreviated to boot.

Bulletin board

Web-based message forum where visitors can read, post, and reply to messages or questions left by other visitors.

Bus

A set of conductors (wires or connectors in an integrated circuit) connecting the various functional units in a computer. There are busses both within the CPU and connecting it to external memory and peripheral devices. The bus width (i.e., the number of parallel connectors) is one factor limiting a computer's performance.

Cache

(Internet browser) The files and graphics saved locally from Web sites you have previously visited.

Card

A circuit board that is usually designed to plug into a connector or slot. See also "Adapter."

CERT

Computer Emergency Response Team. Supports others in enhancing the security of their computing systems; develops standardized set of responses to security problems; provides a central point of contact for information about security incidents; and assists in collecting and disseminating information on issues related to computer security, including information on configuration, management, and bug fixes for systems.

Certificate Revocation List (CRL)

A CRL is a list of certificates (or more specifically, a list of serial numbers for certificates) that have been revoked, and therefore should not be relied upon. A CRL is generated and published periodically, often at a defined interval. The CRL is always issued by the CA which issues the corresponding certificates. All CRLs have a lifetime during which they are valid. During a CRL's validity period, it may be consulted by a PKI-enabled application to verify a certificate prior to use.

Certifying Authority (CA)

This is an entity that issues Digital Signature Certificate to the end users. The digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or assertions made by the private key that corresponds to the public key that is certified. In this model of trust relationships, a CA is a trusted third party that is trusted by both the subject (owner) of the certificate and the party relying upon the certificate.

Cluster

Windows allocates space to files in units called clusters. Each cluster contains from 1 to 64 sectors, depending on the type and size of the disk. A cluster is the smallest unit of disk space that can be allocated for use by files.

CMOS

A part of the motherboard that maintains system variables in static RAM. It also supplies a real-time clock that keeps track of the date, day, and time. CMOS setup is typically accessible by entering a specific sequence of keystrokes during the POST at system start-up.

Cold boot

Starting or restarting a computer by turning on the power supply. See also "Warm boot."

Computer evidence

Computer evidence is quite unique when compared to other forms of documentary evidence. Unlike paper documentation, computer evidence is fragile, and a copy of a document stored in a computer file is identical to the original. The legal "best evidence" rules change when it comes to the processing of computer evidence. Another unique aspect of computer evidence is the potential for unauthorized copies to be made of important computer files without leaving behind a trace that the copy was made. This situation creates problems concerning the investigation of the theft of trade secrets (client lists, research materials, computer-aided design files, formulas, and proprietary software).

Computer forensics

Computer forensics deals with the preservation, identification, extraction, and documentation of computer evidence. The field is relatively new to the private sector but it has been the main stay of technology-related investigations and intelligence gathering in law enforcement and military agencies since the mid-1980s. Like any other forensic science, computer forensics involves the use of sophisticated technology tools and procedures, which must be followed to guarantee the accuracy of the preservation of evidence and the accuracy of results concerning computer-evidence processing. Typically, computer forensic tools exist in the form of computer software. Computer forensic specialists guarantee accuracy of evidence-processing results through the use of time-tested evidence processing procedures and through the use of multiple software tools, developed by separate and independent developers. The use of different tools that have been developed independently to validate results is important to avoid inaccuracies introduced by potential software design flaws and software bugs. It is a serious mistake for computer forensics specialists to put "all of their eggs in one basket" by using just one tool to preserve, identify, extract, and validate the computer evidence. Cross-validation through the use of multiple tools and techniques is standard in all forensic sciences. When this procedure is not used, it creates advantages for defense lawyers who may challenge the accuracy of the software tool used and thus the integrity of the results. Validation through the use of multiple software tools, computer specialists, and procedures eliminates the potential for errors and the destruction of evidence.

Computer investigations

Computer investigations rely on evidence stored as data and the timeline of dates and times that files were created, modified, and last accessed by the computer user. Timelines of activity can be especially helpful when multiple computers and individuals are involved in the commission of a crime. The computer forensics investigator should consider timelines of computer usage in all computer-related investigations. The same is true in computer security reviews concerning potential access to sensitive or trade secret information stored in the form of computer files.

Context menu

Also called a "context-sensitive menu," or a "shortcut menu," a context menu includes the commands that are commonly associated with an object on the screen. To activate an item's context menu, point to it with the screen pointer, then press and release the right mouse button once.

Cookies

(Internet browser) Holds information on the times and dates you have visited Web sites. Other information can also be saved to your hard disk in these text files, including information about online purchases, validation information about you for members-only Web sites, and more.

CPU

Stands for central processing unit, a programmable logic device that performs all the instruction, logic, and mathematical processing in a computer.

Crash

A sudden, usually drastic failure. Can be said of the operating system or a particular program when there is a software failure. A disk drive can crash because of hardware failure.

CyberCash

Used for secure processing of credit-card transactions. It actually takes the payment information and sends it via the banking gateways to obtain real-time approvals for credit cards and checks.

Cryptography

The art of protecting information by transforming it (encrypting it) into an unreadable format, called cipher text. Only those who possess a secret key can decipher (or decrypt) the message into plain text. Cryptography systems can be broadly classified into **symmetric-key systems** and **public-key systems.**

Cryptotoken

Cryptotoken is a security token used to store cryptographic keys for digitally signing thedocuments. They are typically small enough to be carried in a pocket or purse or keychain.
For example : - USB

Data

Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. Any representations such as characters or analog quantities to which meaning is or might be assigned. A representation of facts, concepts, or instructions suitable for communication, interpretation, or processing by humans or computers.

Data-driven attack

A form of attack that is encoded in seemingly innocuous data that is executed by a user's or other software to implement an attack. In the case of firewalls, a data-driven attack is a concern because it may get through the firewall in data form and launch an attack against a system behind the firewall.

Deception

Those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him or her to react in a manner prejudicial to his or her interests.

Decision

In an estimate of the situation, a clear and concise statement of the line of action intended to be followed by the commander as the one most favorable to the successful accomplishment of the mission.

Defragment

As modern file systems are used and files are deleted and created, the total free space becomes split into smaller noncontiguous blocks. Eventually new files being created, and old files being extended, cannot be stored each in a single contiguous block but become scattered across the file system. This degrades performance as multiple seek operations are required to access a single fragmented file. Defragmenting consolidates each existing file and the free space into a contiguous group of sectors. Access speed will be improved as a result of reduced seeking. A nearly full disk system will fragment more quickly. A disk should be defragmented before fragmenting reaches 10%.

Degradation of service

Any reduction (with respect to norms or expectations) in a service processes' reaction or response time, quantitative throughput, or quality parameters. This term is often used to denote the general set of service impairments that at the extreme (total degradation to a "zero state" with respect to the given parameters) constitutes an absolute denial of service. Note that (owing to operational constraints such as "time before timing out" settings) a disruptive tactic capable of only degrading service may result in a complete denial of said service from the perspective of the end user.

Denial of service

Actions that prevent any part of an automated information system (AIS) from functioning in accordance with its intended purpose. Denial of service attacks may include denying services or processes limited to one host machine. However, the term is most often invoked to connote action against a single host (or set of hosts), which results in the target's inability to perform services for other users- particularly over a network. One may consider denial of service to be the extreme case of degradation of service in which one or more normal functional parameters (response, throughput) get "zeroed out," at least as far as the end user is concerned. It is important to note that denial is delineated with respect to whether the normal end user(s) can exploit the system or network as expected. Seen in this light, denial (like degradation) is descriptive of a functional outcome and is not therefore definitive with respect to cause (tactics effecting said result). Forms of attack not geared to denial per se may lead to denial as a corollary effect (when a system administrator's actions in response to an intrusion attempt lead to a service outage). As such, denial of service is not a good criterion for categorizing attack tactics.

Denial time

The average length of time that an affected asset is denied to the organization. The temporal extent of operational malaise induced by a denial of service attack.

Digital Signature Certificates (DSC)

Certificates serve as identity of an individual for a certain purpose, e.g. a driver's license identifies someone who can legally drive in a particular country. Likewise, a Digital Signature Certificate (DSC) can be presented electronically to prove your identity or your right to access information or services on the Internet.

Directory

An index into the files on your disk. It acts as a hierarchy and you will see the directory represented in Windows looking like manila folders.

Disk space

The amount of storage space you're allocated to use on the server; also server space and Web space. The more disk space you have, the bigger your Web site can be. It's used to store everything related to your Web site such as your regular html files, images, multimedia files, anonymous ftp files, POP mail messages, CGI scripts, and any other files that make up your Web site.

DMA

Stands for direct access memory. DMA is a fast way of transferring data within a computer. Most devices require a dedicated DMA channel (so the number of DMA channels that are available may limit the number of peripherals that can be installed).

Domain name registration

A domain name is a textual address that is a unique identifier for your Web site and that corresponds to your site's numerical Internet protocol (IP) address and is usually related to your business, such as www.acmecatapults.com.

DRAM

Dynamic random access memory (see also "SDRAM"). A type of memory used in a PC for the main memory (such as your 32 Mbytes of RAM). Dynamic refers to the memory's memory of storage-basically storing the charge on a capacitor. Specialized types of DRAM (such as EDO memory) have been developed to work with today's faster processors.

Driver

A program designed to interface a particular piece of hardware to an operating system or other software.

Electromagnetic intrusion

The intentional insertion of electromagnetic energy into transmission paths in any manner, with the objective of deceiving operators or causing confusion.

Electronic warfare

Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or attack the enemy. Also called EW.

Electronics intelligence (ELINT)

Technical and geolocation intelligence derived from foreign non-communications, electromagnetic radiations emanating from sources other than nuclear detonations or radioactive sources.

Electronics security

The protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from their interception and study of non communications electromagnetic radiations (radar). This term is also (more loosely) used to connote the topical area or task specialization focusing on achieving this type of protection.

Electro-optical intelligence

Intelligence other than signals intelligence derived from the optical monitoring of the electromagnetic spectrum from ultraviolet (0.01 micrometers) through far infrared (1,000 micrometers).

Email accounts (POP)

Your email boxes on a server that can be accessed directly to retrieve your mail using such programs as Outlook Express and Netscape Mail. Each POP3 has its own password to ensure privacy, so each of your employees can have their own email address.

Email aliases

Your main POP account for your domain allows the system to capture any name that may be sent to your domain name. This means as long as the @yourdomain.com is proper, any name in front of it will be delivered to your main POP account. Each alias can be forwarded or redirected to any other address of your choice.

Email forwarding

Any email address at your domain may be configured to forward to any other real internet email address. For example, sales@yourname.com can forward to you@aol.com if you like.

Executable

A binary file containing a program in machine language that is ready to be executed (run). Windows machines use the filename extension .exe for these files.

Expansion card

An integrated circuit card that plugs into an expansion slot on a motherboard to provide access to additional peripherals or features not built into the motherboard. See also "Adapter."

Extract

To return a compressed file to its original state. Typically, to view the contents of a compressed file, you must extract it first.

File

A collection of data grouped into one unit on a disk.

File allocation table

(FAT or FAT32) The FAT links together all of the clusters belonging to each file, no matter where they are on disk. The FAT is a critical file: you should be sure to back it up regularly. FAT32 is a newer type of FAT, which was designed to handle large hard disks. The older FAT (FAT16) can only support partitions up to two gigabytes in size. FAT32 can handle partitions that are thousands of gigabytes.

File system

A system for organizing directories and files, generally in terms of how it is implemented in the disk-operating system.

Firewall

A metaphorical label for a set of hardware and software components protecting system resources (servers, LANs) from exogenous attack via a network (from Internet users) by intercepting and checking network traffic. The mix of hardware and software accomplishing firewall operations can vary. For LAN installations of any size, the typical approach is to install one or more computers positioned at critical junctures (gateways) and dedicated to the firewall functions. It is typically the case that such installations are configured such that all external connections (modems, ports) are outside the firewall (with respect to its domain of protection), or at least abut it on its external face. The firewall's own internal connection into the protected domain is typically the focus of monitoring functions. A firewall is also a system or combination of systems that enforces a boundary between two or more networks or a gateway that limits access between networks in accordance with local security policy. The typical firewall is an inexpensive micro-based Unix box kept clean of critical data, with numerous modems and public network ports on it but only one carefully watched connection back to the rest of the cluster.

Firmware

Software contained in a read-only memory (ROM) device.

Fork bomb

A disruptive piece of code directed toward a Unix-based system that causes runaway "forking" (splitting or replication) of operating system processes to degrade or (if saturation is achieved) deny that target system's operations. Code that can be written in one line of code on any Unix system; used to recursively spawn copies of itself, explode, and eventually eat all the process table entries. It effectively locks up the system.

Fragmentation

The state of having a file scattered around a disk in pieces rather than existing in one contiguous area of the disk. Fragmented files are slower to read than unfragmented files.

FTP account

Used to upload and download files to and from your Web site. You have unlimited access to your account 24 hours a day. You'll need to have FTP client software.

Hacker

The label "hacker" has come to connote a person who deliberately accesses and exploits computer and information systems to which he or she has no authorized access. 0riginally, the term was an accolade for someone highly motivated to explore what computers could do or the limits of his or her technical skills (especially in programming). "A great hack" was a common compliment for an especially cunning or innovative piece of software code. The term cracker was then reserved for people intruding into computer or information systems for the thrill of it (or worse). 0ver time, cracker faded from usage and hacker came to subsume its (unfortunate) connotations.

Hash Function

A cryptographic hash function is a deterministic procedure that takes an arbitrary block of data and returns a fixed-size bit string, the (cryptographic) hash value, such that an accidental or intentional change to the data will change the hash value. The data to be encoded is often called the "message", and the hash value is sometimes called the message digest or digest or hash.

Head

A small electromagnetic device inside a drive that reads, writes, and erases data on the drive's media.

Heat Sink

A mass of metal attached to a chip carrier or socket for the purpose of dissipating heat.

Hijacking

A term (typically applied in combination with another) to connote an action to usurp activity or interactions in progress. Most commonly used for those tactics that allow an intruder to usurp an authorized user's session for his or her own ends.

History

(1nternet browser) Stores the internet addresses
(URLs) of the Web sites you have visited.

I/O Port

110 stands for input1output. 110 is the communication between a computer and its user, its storage devices, other computers (via a network), or the outside world. The 110 port is the logical channel or channel endpoint in an 110 communication system.

IDE

Stands for integrated drive electronics. Describes a hard disk with the disk controller integrated within it. See also "EIDE".

Indirect information warfare

Changing the adversary's information by creating phenomena that the adversary must then observe and analyze.

Information

Facts, data, or instructions in any medium or form. The meaning that a human assigns to data by means of the known conventions used in their representation. In intelligence usage, unevaluated material of every description that may be used in the production of intelligence.

Information Age

A label generally used to connote the present or prospective era in which information technology (IT) is the dominant technical artifact. The future time period when social, cultural, and economic patterns will reflect the decentralized, nonhierarchical flow of information; contrast this to the more centralized, hierarchical, social, cultural, and economic patterns that reflect the Industrial Age's mechanization of production systems.

Information Age warfare

That subset of war-making that uses information technology as a tool to impart combat operations with unprecedented economies of time and force. This is exemplified by a cruise missile on precision force projection.

Information attack

Directly corrupting information without visibly changing the physical entity within which it resides. In the wake of an information attack, an information function is indistinguishable from its original state except through inspecting its data or instructions.

Information-based warfare (IBW)

Synonym for information warfare. An approach to armed conflict focusing on managing and using information in all its forms and at all levels to achieve a decisive military advantage, especially in the joint and combined environment.

Information collection

That aspect of IW activities concerned with the acquisition of data. An organization needs a variety of information to support its operations. Information collection includes the entry points for information into an organization from both internal and external sources. Issues include quantity (completeness), quality (accuracy), and timeliness of this information. Business examples of collection systems include point-of-sale (POS) systems, market surveys, government statistics, and internal management data. Military examples of collection systems include tactical radars and other sensors.

Information compromise

That class or type of IW threat that involves a competitor gaining access to an organization's proprietary data.

Information denial

Measures beyond normal protection to specifically target an adversary's collection systems. There are two types of denial: direct attacks on the adversary's information systems, and providing misinformation to its systems to deceive and induce the adversary to take actions that are not to its advantage. For the military, direct attacks include electronic warfare (jamming) of sensors and radio links. Besides direct attacks, there are safer ways to corrupt an adversary's databases. These rely on providing false information to the targeted competitor's collection systems to induce this organization to make bad decisions based on this faulty information.

Information destruction

That class or type of IW threat to one's data assets that involves the loss of these data (or loss of access to these data) as the result of a hostile attack by an adversary.

Information dominance

In warfare, an operational advantage obtained through superior effectiveness of informational activity (acquisition and processing of data, information, and/or knowledge), to the extent that this advantage is demonstrated in practice through superior effectiveness of instrumental activity.

Information dominance warfare (IDW)

The subcategory of information warfare (IW) aimed at leveraging data, information, and knowledge to tactical and strategic advantage, as opposed to leveraging the media, channels, and vehicles of information transfer and processing. The goal of IDW is to achieve information dominance.

Information security (INFOSEC)

The protection of unauthorized access to or modification of information, whether in storage, processing, or transit, and against the denial of service to authorized users or the provision of service to unauthorized users, including those measures necessary to detect, document, and counter such threats.

Information superiority

That degree of dominance in the information domain that permits the conduct of operations without effective opposition. Information superiority combines the capabilities of intelligence, surveillance, reconnaissance (ISR) and command, control, communications, computers, and intelligence (C4I) to acquire and assimilate information needed to effectively employ our own forces to dominate and neutralize adversary forces. It includes the capability for near-real-time awareness of the location and activity of friendly, adversary, and neutral forces throughout the battlespace and a seamless, robust C4I network linking all friendly forces that provides common awareness of the current situation.

Information system(s) (INFOSYS)

The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information.

Information terrorism

An ill-defined term (as yet) invoked to connote cyberspace mischief undertaken with intentions or ramifications analogous to the fear- inducing physical attacks one associates with terrorist activity.

Information war

Activities intertwined with, and superimposed on, other military operations, exploiting data and information in support of traditional military tasks such as command and control.

Information warfare (IW)

The broad class of activities aimed at leveraging data, information, and knowledge in support of military goals. Subcategories of information warfare can be differentiated into two general classes:

(a) those aimed at leveraging the vehicles of information transfer or processing (information systems warfare [ISW]) and (b) those aimed at leveraging the informative content or effect of such systems.

IRQ

Stands for interrupt request. IRQ is the name of the hardware interrupt signals that PC peripherals (such as serial or parallel ports) use to get the processor's attention. Because interrupts usually cannot be shared, devices are assigned unique IRQ addresses that enable them to communicate with the processor. Peripherals that use interrupts include LAN adapters, sound boards, scanner interfaces, and SCSI adapters.

Java chat rooms

Real-time chat via a Java applet that allows visitors to your Web site to engage in live discussion with you or with each other. You can provide it just for fun or use it to interact with your customers in real-time.

Jumper

A small, plastic-covered metal clip that slips over two pins protruding from a circuit board. When in place, the jumper connects the pins electronically and closes the circuit, turning it on.

Kernel

An essential part of the operating system, responsible for resource allocation, low-level hardware interfaces, security, and more.

Keystroke monitoring

A form of user surveillance in which the actual character-by-character traffic (that user's keystrokes) are monitored, analyzed, and logged for future reference. A specialized form of audit trail software, or a specially designed device, that records every key struck by a user and every character of the response that the host computer returns to the user.

Knowledge

The state or mechanism ascribed to a system to explain complex mediation between effective acquisition of data from, and effective action in, an operational environment. This approach to knowledge explicitly ties it to the processes of both education and inaction with respect to the given operational environment and hence links it to one or more specific actors in that given domain. These connections explain the IW literature's claims that knowledge is active and must be possessed if it is to exist let alone be useful.

Knowledge-based warfare

The ability of one side to obtain essential and key elements of truth while denying these same elements of truth to the other side. The key attributes of knowledge-based warfare are timely, high fidelity, comprehensive, synthesized, and visual data. The end game is a complete pictorial representation of reality that the decision maker can tune to his or her unique needs at any given time. This picture must include both blue (one side) and red data (the other side), although this advanced concept technology demonstration (ACTD) concentrates on the provision of blue data only.

Knowledge dominance

In warfare, an operational advantage (vis-a-vis an adversary) in exploiting information to guide effective action. This is the goal of information dominance.

Leapfrog attack

Any form of intrusion or attack accomplished by exploitation of data or information obtained on a site or server other than the attack's target.

Letter bomb

Malicious or disruptive code delivered via an email message (or an attachment to said message). A piece of email containing live data intended to do malicious things to the recipient's machine or terminal. Under UNIX, a letterbomb can also try to get part of its contents interpreted as a shell command to the mailer. The results of this could range from silly to tragic.

Logic bomb

The term for a mischievous or destructive piece of software (virus, Trojan horse) that lies resident on the victim computer or system until triggered by a specific event (onset of a predetermined date or set of system conditions).

Lost cluster chain

A cluster on disk that is not registered as free but does not have any known data in it.

Mail bomb

Unlike a logic bomb (a thing), mail bomb is a verb used to connote deliberately deluging a target system or host with email messages for purposes of harassment, degradation of service, or even denial of service.

Mail storm

What the target system or users see when being mail bombed. Any large amount of incoming email sufficient to disrupt or bog down normal local operations. What often happens when a machine with an Internet connection and active users reconnects after extended downtime-a flood of incoming mail that brings the machine to its knees.

Message

Any thought or idea expressed briefly in a plain or secret language and prepared in a form suitable for transmission by any means of communication.

Mirror image backups

Also referred to as bit-stream backups, these involve the back up of all areas of a computer hard disk drive or other type of storage media (Zip disks, Iaz disks, etc.). Mirror image backups exactly replicate all sectors on a given storage device. Thus, all files and ambient data storage areas are copied. Such backups are sometimes referred to as "evidence grade backups" and they differ substantially from standard file backups and network server backups.

Misuse detection

The class of intrusion detection tactics that proceed on the presumption that problematical intrusions (attacks) can be positively characterized and that detection of their characteristic profile is sufficient for identifying potential threats.

Mockingbird

A computer program or process that mimics the legitimate behavior of a normal system feature (or other apparently useful function) but performs malicious activities once invoked by the user.

Monthly traffic (bandwidth)

The sum of outward-bound or inward-bound Web pages, files, email, and anonymous FTP traffic. Each time a Web page, image, audio, video, or other element of your Web site is accessed by your visitor, traffic is generated.

Motherboard

The "heart" of your PC-it handles system resources (IRQ lines, DMA channels, I10 locations), as well as core components such as the CPU and all system memory. It accepts expansion devices such as sound and network cards and modems.

Network spoofing

In network spoofing, a system presents itself to the network as though it were a different system (system A impersonates system B by sending B's address instead of its own). The reason for doing this is that systems tend to operate within a group of other "trusted" systems. Trust is imparted in a one-to-one fashion; system A trusts system B (this does not imply that system B trusts system A). Implied with this trust is that the system administrator of the trusted system is performing his or her job properly and maintaining an appropriate level of security for his or her system. Network spoofing occurs in the following manner: if system A trusts system B and system C spoofs (impersonates) system B, then system C can gain otherwise denied access to system A.

Network worm

A worm that migrates across platforms over a network by copying itself from one system to another by exploiting common network facilities, resulting in execution of the (replicated) worm on that system and potentially others.

NTFS

Windows NT file system.

Open-source intelligence (OSINT)

Information of potential intelligence value that is available to the general public.

Operational intelligence

Intelligence that is required for planning and conducting campaigns and major operations to accomplish strategic objectives within theaters or areas of operations.

Operations security (OPSEC)

A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities.

Packet sniffer

A device or program that monitors the data traveling between computers on a network.

Packet sniffing

Packet sniffing is a technique in which attackers surreptitiously insert a software program at remote network switches or host computers. The program monitors information packets as they are sent through networks and sends a copy of the information retrieved to the hacker. By picking up the first 125 keystrokes of a connection, attackers can learn passwords and user identifications, which, in turn, they can use to break into systems.

Partition

A logical section of a disk. Each partition normally has its own file system.

Partition table

A 64-byte data structure that defines the way a PC's hard disk is divided into logical sectors known as partitions. The partition table describes to the operating system how the hard disk is divided. Each partition on a disk has a corresponding entry in the partition table. The partition table is always stored in the first physical sector of a disk drive.

Passive attack

A form of attack in which data is released (captured or obtained) from the target system. Attack that does not result in an unauthorized state change, such as an attack that only monitors or records data.

Passive threat

The threat of unauthorized disclosure of information without changing the state of the system. A type of threat that involves the interception, not the alteration, of information.

Password cracking/password theft

Password cracking is a technique used to surreptitiously gain system access by using another user's account. Users often select weak passwords. The two major sources of weakness in passwords are easily guessed passwords based on knowledge of the user (for example, wife's maiden name) and passwords that are susceptible to dictionary attacks (brute-force guessing of passwords using a dictionary as the source of guesses). Password cracking and theft is a technique in which attackers try to guess or steal passwords to obtain access to computer systems. Attackers have automated this technique; rather than attackers trying to guess legitimate users' passwords, computers can very efficiently and systematically do the guessing. For example, if the password is a dictionary word, a computer can quickly look up all possibilities to find a match. Complex passwords comprised of alphanumeric characters are more difficult to crack. However, even with complex passwords, powerful computers can use brute force to compare all possible combinations of characters until a match is found.

Password sniffing

A form of sniffing that entails sampling specific portions of the data stream during a session (collecting a certain number of initial bytes where the password can be intercepted in unencrypted form on common Internet services) so as to obtain password data that can then be exploited.

Path

A location of a file. The path consists of directory or folder names, beginning with the highest-level directory or disk name and ending with the lowest-level directory name. A path can identify a drive (C:\), a folder (C:\Temp), or a file (C:\Windows\ftp.exe).

Penetration

With regard to IW, a successful attack-the ability to obtain unauthorized (undetected) access to files and programs or the control state of a computer system.

Penetration signature

The description of a situation or set of conditions in which a penetration could occur or of system events that in conjunction can indicate the occurrence of a penetration in progress.

Peripheral

Any part of a computer other than the CPU or working memory (RAM and ROM). For example, disks, keyboards, monitors, mice, printers, scanners, tape drives, microphones, speakers, and other such devices are peripherals.

Phracker

Individual who combines phone phreaking with computer hacking. Formed by a play on both phreaker and hacker.

Phreak/phone phreak

A term for hacking or cracking-type exploitation directed at the telephone system (as opposed to the data communications networks). When the intrusion or action involves both telephone and data communications networks, that portion of the intrusion activity directed toward manipulating the telephone system is typically called phreaking.

Phreaker

Individual fascinated by the telephone system. Commonly, an individual who uses his or her knowledge of the telephone system to make calls at the expense of another.

Plug-and-Play (PnP)

A hardware and software specification developed by Intel that allows a PnP system and a PnP adapter to configure automatically. PnP cards generally have no switches or jumpers but are configured via the PnP system's BIOS or with supplied software for non-PnP computers.

POST

Stands for power-on self test. Each time a PC initializes, the BIOS executes a series of tests collectively known as the POST. The test checks each of the primary areas of the system, including the motherboard, video system, drive system, and keyboard, and ensures that all components can be used safely. If a fault is detected, the POST reports it as an audible series of beeps or a hexadecimal code written to an I1O port.

Public - Key (Asymmetric Key) Cryptography

This system is based on pairs of keys called public key and private key. The public key is published and known to everyone while the private key is kept secret with the owner. The need for a sender and a receiver to share a secret key and trust some communications channel is eliminated.

Public Key Infrastructure (PKI)

PKI is a combination of software, encryption technologies, and services that enable enterprises to protect the security of their communications and business transactions over networks by attaching so-called "digital signatures" to them.

RAM

Random Access Memory (see also "DRAM," "SDRAM"). A data-storage device for which the order of access to different locations does not affect the speed of access. This is in contrast to magnetic disk or magnetic tape, where it is much quicker to access data sequentially because accessing a non-sequential location requires physical movement of the storage medium rather than just electronic switching. The most common form of RAM in use today is built from semiconductor integrated circuits, which can either be static (SRAM) or dynamic (DRAM).

Random text displayer

Visitors see random messages you have saved in a text file, such as famous quotes or announcements. Generally, the visitor will see a different message every time they visit the site.

Real Audio/Video

A client-server based system where both the browser and server must have real audio/video components to provide streaming media to visitors at a Web site without waiting for the clip to download.

Registration Authority (RA)

This is an entity within the CA that acts as the verifier for the Certifying Authority before a Digital Signature Certificate is issued to a requestor. The Registration Authority (RA) processes user requests, confirm their identities, and induct them into the user database.

Retro-virus

A virus that waits until all possible backup media are also infected, so that it is not possible to restore the system to an uninfected state.

Risk

With specific regard to data or information systems-accidental or unpredictable exposure of information, or violation of operations integrity because of the malfunction of hardware or incomplete or incorrect software design.

ROM

Read-only memory. A type of data-storage device that is manufactured with fixed contents. The term is most often applied to semiconductor-integrated circuit memories. ROM is inherently nonvolatile storage-it retains its contents even when the power is switched off, in contrast to RAM. It is used in part for storage of the lowest level bootstrap software (firmware) in a computer.

Root Certifying Authority of India (RCAI)

This entity is created under CCA and is responsible for issuing Public Key Certificates to Licensed Certifying Authorities. This serves as the root of the trust chain in India. The requirements fulfilled by the RCAI include the following:

- The licence issued to the CA is digitally signed by the CCA.
- All public keys corresponding to the signing private keys of a CA are digitally signed by the CCA.
- That these keys are signed by the CCA can be verified by a relying party through the CCA's website or CA's own website.

Scripts

Scripts are programs written to run with Web pages and perform a specific task in response to visitor actions such as clicking a button. For example, a Perl script counts the visits to the page, and a JavaScript script makes the buttons change colors when you put your mouse pointer over them. Scripts can be written in Perl, Java, JavaScript, VBScript, and a dozen other programming languages.

SCSI

Stands for small computer system interface. A standard that allows multiple devices to be connected in daisy-chain fashion.

SDRAM

Stands for synchronous dynamic random access memory (see also "DRAM"). SDRAM incorporates new features that make it faster than standard DRAM and EDO memory.

Search engine

A CGI script that allows visitors to perform keyword searches of a Web site.

Secret key (Symmetric/Conventional) cryptography

This is a system based on the sender and receiver of a message knowing and using the same secret key to encrypt and decrypt their messages. One weakness of this system is that the sender and receiver must trust some communications channel to transmit the secret key to prevent from disclosure. This form of cryptography ensures data integrity, data authentication and confidentiality.

Sector

The tracks on a disk are divided into sectors. Clusters contains from 1 to 64 sectors.

Secure server (SSL)

One method of ensuring that information entered through your Web site is protected. Information submitted via a secure form is sent to the server in encrypted mode. This is most commonly used for credit card transactions.

Security

Measures taken by a military unit, an activity, or installation to protect itself against all acts designed to, or which may, impair its effectiveness.

Security audit

A search through a computer system for security problems and vulnerabilities.

Security breach

A violation of controls of a particular information system such that information assets or system components are unduly exposed.

Security classification

A category to which national security information and material is assigned to denote the degree of damage that unauthorized disclosure would cause to national defense or foreign relations of the United States and to denote the degree of protection required.

Server

A special computer designed for the Internet or another network, usually far more powerful than a regular desktop computer, that has a full-time direct connection to the Internet. Some servers even have two or more processors working together. Servers run special software called Web server software, which enables them to receive requests and deliver files to other computers across the Internet.

Server side includes (SSI)

Allows the server to understand and respond to special page commands. As an example, if you had a footer you wanted on all your pages that may change from time to time, you can create a text file with the desired footer and place it in your document. On each page you put a simple include to read the file and place it at the bottom of the desired pages. Changing the footer on all your pages would be as simple as changing the one text file.

Session hijacking

Taking over an authorized user's terminal session, either physically when the user leaves his or her terminal unattended or electronically when the intruder carefully connects to a just-disconnected communications line.

Shopping cart

Keeps track of what your customers have ordered online as they add and remove items. When a customer is ready to check out, the program tallies the order for processing and takes their credit card and other information.

Signal

As applied to electronics, any transmitted electrical impulse.

Signal security (SIGSEC)

A generic term that includes both communications security and electronic security.

Signals intelligence (SIGINT)

A category of intelligence composed of-either individually or in combination-all communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, however transmitted.

Site submission

Submits your site information to a database of over 1,900 search engines, link engines, and directories.

Situation Awareness (SA)

Sometimes termed "situational awareness." The perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future. This term is broadly used to denote the state of awareness that a subject (operator, pilot) has in the course of a task at a given point in time. As such, it connotes a degree of orientation to those circumstances at that point in time- particularly those that are germane to the task itself. The term is also (more loosely) used to connote such a state of awareness or orientation with respect to multiple actors or organizational units. As such, the notion of situation awareness maps straightforwardly onto the orientation phase of the OODA Loop.

Slot

A physical connector on a motherboard to hold an expansion card, SIMM, DIMM, or a processor card in place.

Sniff/sniffing

The act of surreptitiously monitoring data streams so as to intercept and capture exploitable information.

Sniffer

A tool used to intercept potentially exploitable data from the traffic on a network. A program to capture data across a computer network. Used by hackers to capture user-ID names and passwords. A software tool that audits and identifies network traffic packets.

Social engineering

A term for personal (social) tactics employed in support of attempts to achieve unauthorized access to a computer or information system. This is something of a catch-all category for any tricks used to obtain the intended access or to obtain information critical to achieving that access.

Spam

The act of bombarding a target (system, Usenet news group, set of email addresses) with sufficient volume of data (or a volume of sufficiently massive data items) such that degradation or even denial of service is achieved. This term is also pejoratively applied to describe the perceived harassment of receiving profligately broadcast data (junk email advertising). To crash a program by overrunning a fixed-site buffer with an excessively large input data. Also, to cause a person or newsgroup to be flooded with irrelevant or inappropriate messages.

System registry

The system configuration files used by Windows 2000, XP, 2003, and NT to store settings about user preferences, installed software, hardware and drivers, and other settings required for Windows to run correctly. The system updates the registry every time you add new hardware or a new program to your system. When the registry becomes "broken," it can cause serious system problems.

Tactical internet

A battlefield communication system networked together using commercially based internet protocols.

Technical attack

An attack that can be perpetrated by circumventing or nullifying hardware and software protection mechanisms, rather than by subverting system personnel or other users.

Technical intelligence (TECHINT)

Intelligence derived from exploitation of foreign materiel, produced for strategic, operational, and tactical level commanders. Technical intelligence begins when an individual service member finds something new on the battlefield and takes the proper steps to report it. The item is then exploited at succeedingly higher levels until a countermeasure is produced to neutralize the adversary's technological advantage.

Telnet account

Telnet allows real-time access to the command line of your server to run programs and install and configure scripts. Most CGI scripts can be installed without Telnet unless you need it for debugging purposes.

Terminal hijacking

Allows an attacker on a certain machine to control any terminal session that is in progress. An attack hacker can send and receive terminal I10 while a user is on the terminal.

Terminator

Most commonly found in relation to a SCSI chain, this prevents the reflection or echoing of signals that reach the ends of the SCSI bus. Usually terminators are hardware circuits or jumpers.

Time bomb

A logic bomb that is specifically triggered by a temporal event (a predetermined date or time). A logic bomb that is triggered by reaching some preset time, either once or periodically. A variant of the trojan horse, in which malicious code is inserted to be triggered later.

Trap door

A hidden software or hardware mechanism used to circumvent security control.

Trojan horse

An independent program that, when called by an authorized user, performs a useful function but also performs unauthorized functions, often usurping the privileges of the user.

Unallocated file space

Unallocated file space and file slack are both important sources of leads for the computer forensics investigator. The data-storage area in a factory-fresh hard disk drive typically contains patterns of sectors that are filled with patterns of format characters. The same format pattern is sometimes used in the format of hard disk drives, but the format patterns can consist of essentially any repeat character as determined by the factory test machine that made the last writes to the hard disk drive. The format pattern is overwritten as files and subdirectories are written in the data area.

Unzip

To unzip is to extract (see "Extract") a Zip archive.

Video adapter

An expansion card or chip set built into a motherboard that provides the capability to display text and graphics on the computer's monitor. If the adapter is part of an expansion card, it also includes the physical connector for the monitor cable. If it is a chip set on the motherboard, the video connector will be on the motherboard also.

Virus

The generic label for a unary set of code that is designed to cause mischief or other subversive effect in a target computer system.

Vulnerability

With specific regard to IW-a known or suspected flaw in the hardware or software or operation of a system that exposes the system to penetration or its information to accidental disclosure.

War dialer

A cracking tool, a program that calls a given list or range of numbers and records those that answer with handshake tones (and so might be entry points to computer or telecommunications systems).

Warfare

The set of all lethal and non-lethal activities undertaken to subdue the hostile will of an adversary or enemy. The distinction between this and war ties into the delineation of information warfare as an activity, which could or should be conducted outside the situational frame of war itself.

Warm boot

Rebooting a system by means of a software command as opposed to turning the power off and on. See also "Cold boot."

Web-based Telnet

Invoke a telnet session directly from your Web browser. There's no need for any other applications or software.

Windows swap files

Windows swap files are relied on by Windows, Windows 2000, Windows XP, and Windows 2003 to create "virtual memory" (using a portion of the hard disk drive for memory operations). The storage area is important to the computer forensics specialist for the same reason that file slack and unallocated space are important (large volumes of data exist for which the computer user likely has no knowledge). Windows swap files can be temporary or permanent, depending on the version of Windows involved and settings selected by the computer user. Permanent swap files are of more interest to a computer forensics specialist because they normally store larger amounts of information for much longer periods of time.

Wizard

A wizard is a series of dialog boxes that guides you step by step through a procedure.

World Wide Web

The World Wide Web, or WWW, is the part of the Internet that you use to view a particular Web page. The Web is just a set of protocols, or standards, for transferring data from one computer to another; just one aspect of the Internet, but by far the most popular. Telnet, FTP, Veronica, and Archie are some other Internet data-transfer protocols. Without protocols, computers wouldn't be able to communicate with or understand each other.

Worm

A class of mischievous or disruptive software whose negative effect is primarily realized through rampant proliferation (via replication and distribution of the worm's own code). Replication is the hallmark of the worm. Worm code is relatively host-independent, in that the code is self-contained enough to migrate across multiple instances of a given platform, or across multiple platforms over a network (network worm). To replicate itself, a worm needs to spawn a process; this implies that worms require a multitasking operating system to thrive. A program or executable code module that resides in distributed systems or networks. It will replicate itself, if necessary, in order to exercise as much of the systems' resources as possible for its own processing. Such resources may take the form of CPU time, I10 channels, or system memory. It will replicate itself from machine to machine across network connections, often clogging networks and computer systems as it spreads.

Zip

To zip a file is to compress it into an archive so that it occupies less disk space.

Zip archive

An archive of one or more Zip-compressed files. When used as a noun, Zip is typically capitalized. Compressed files can come in many formats besides Zip.

Zip file

A Zip archive that Windows presents as a single file. In general, the contents cannot be accessed unless the archive is decompressed.

Annexure II

Acronyms

ADKAR	Awareness, Desire, Knowledge, Ability, Reinforcement
BCA	Business Case Analysis
BOO	Build Own Operate
BOOT	Build Own Operate Transfer
BPR	Business Process Re-engineering
CA	Certified Authority
CCTNS	Crime & Criminal Tracking Network
CDSW	Custom Developed Software
CERT	Computer Emergency Response Team
CFST	Citizen Friendly Services of Transport Department
COTS	Commercial off the Shelf
CSC	Citizen Service Center
DAR&PG	Department of Administrative Reforms & Public Grievances
DFSS	Definition for Six Sigma
DISNIC	District Information System of National Informatics Center
DIT	Department of Information Technology
DMIC	Define, Measure, Analyze, Improve, Control
DPR	Detailed Project Report
ECV	Estimated Contract Value
EOI	Expression of Interest
ERP	Enterprise Resource Planning
FBS	Fixed Budget Selection
G2B	Government to Business
G2C	Government to Citizen
G2E	Government to Employee
G2G	Government to Government
GFR	General Financial Rules
GPR	Government Process Re-engineering
GPS	Global Positioning System
ICR	Intelligent Character Recognition
ICT	Information & Communication Technology
ILIS	Integrated Land Information System

IPR	Intellectual Property Right
IRR	Internal Rate of Return
ISDN	Integrated Services Digital Network
ISS	Information System Security
ITAA	IT Act Amendment
ITES	IT enabled Services
JV	Joint Venture
KPI	Key Performance Indicator
LAN	Local Area Network
LCS	Least Cost Selection
LSIP	Large Scale Interactive Process
M&E	Monitoring & Evaluation
MCA	Ministry of Corporate Affairs
MIS	Management Information System
MMP	Mission Mode Project
MSA	Measurement System Analysis
NeGD	National e-Governance Division
NeGP	National e-Governance Plan
NICNET	National Informatics Center Network
NISG	National Institute for Smart Government
NLSA	National Level Service Agency
NPV	Net Present Value
NSDG	National Service Delivery Gateway
OCR	Optical Character Recognition
OMR	Optical Mark Recognition
PDA	Personal Digital Assistant
PeMT	Project e-Governance Mission Team
PKI	Public Key Infrastructure
PMC	Project Management Committee
PMU	Project Management Unit
PPP	Public Private Partnership
PSC	Public Sector Comparator
QBS	Quality Based Selection
QCBS	Quality & Cost Based Selection
RA	Registration Authority
RAO	Rapid Application Development

RFID	Radio Frequency Identification
RFP	Request for Proposal
RFQ	Request for Qualification
ROC	Registrar of Companies
ROI	Return on Investment
SAP	Service Access Provider
SAS	Software As Service
SDA	State Designated Agency
SDC	State Data Center
SDLC	Software Development Lifecycle
SeMT	State e-Governance Mission Team
SLA	Service Level Agreement
SLM	Service Level Management
SLO	Service Level Objective
SMART	Simple, Moral, Accountable, Responsive, Transparent
SOA	Service Oriented Architecture
SoW	Scope of work
SP	Service Provider
SPV	Special Purpose Vehicle
SSDG	State e-Governance Service Delivery Gateway
STOC	Standards Testing Certification
SWAN	State Wide Area Network
TCV	Tender Contract Value
UAT	User Acceptance Testing
UCID	Unique Company Identification Number
UID	Unique Identification Number
UNCITRAL	United Nations Commission on International Trade Law
VLE	Village Level Entrepreneur
WAN	Wide Area Network