CHAPTER 5

FRAMEWORK FOR E-GOVERNANCE APPLICATIONS
CHAPTER 5

FRAMEWORK FOR E-GOVERNANCE APPLICATIONS

5.1 E-GOVERNANCE FRAMEWORK

5.1.1 INTRODUCTION

In day to day activities e-Governance became part of every walk of life and its roots were deeply penetrated into the society that without it, imagining comfortable human activities is difficult. It provides effective and efficient services, increasing productivity extending several benefits to society and hence the governments of various countries introduced e-Governance applications. The growing importance of e-Governance, spreading its branches in varied fields is going out of control sprouting new issues leading to unsuccessful penetration.
5.1.2 MAJOR ISSUES

Issues of e-Governance can be classified under three heads Government to Citizen (G2C) issues, Government to Business (G2B) issues and Government to Government (G2G) issues.

A. GOVERNMENT-TO-CITIZENS ISSUES

Government to Citizen Services includes all the interactions between a government and its citizens that take place electronically using network communications implementing government policies. The issues in implementation of G2C applications are because of population explosion, poverty, illiteracy, villages, corruption, telecom problems, unaffordable cost of internet, funding problems, unreliability towards e-Governance, shortage of technical skills, computer illiteracy, lack of human touch, economic and financial issues and online support.

B. GOVERNMENT-TO-BUSINESS ISSUES

Government interaction with business organizations is dealt by G2B services. The issues in implementations are integrated service requirement, lack of information, training programs, civil servants programs, start-up services, licensing checkups, business funding, channel conflicts, cyber mediation, hyper mediation problems, right pricing problems, personalization failures, Security issues, incorrect revenue model, legal issues, taxation issues, unaffordable cost of net, computer illiteracy.

C. GOVERNMENT TO GOVERNMENT ISSUES

The G2G category consists of electronic commerce activities between units of government, including those within one governmental body and those between different governments. The
various issues related with G2G are improper coordination among departments, political interference, re-engineering, lack of empowered leaders, scaling, infrastructure components, capacity building and lack of close monitoring of activities, time delays, and domain specialists’ participation, various administrative issues, geographical issues and economic issues.

The above issues can be minimized by implementing the proposed e-Governance framework activities.

**5.1.3 FRAMEWORK ACTIVITIES**

In order to control and minimize the issues of G2C, G2B and G2G, a framework of activities are to be undertaken. The e-governance framework components are planning, audit on services, social audit, infrastructure audit, professional audit, software audit, software down time, budgeting the total projects. The framework elements are depicted in the following figure and discussed in detail in the succeeding session.
Problematic e-Governance Sphere

Problems with G2C
- Audit on Services
- Planning
- Social Audit

Problems with G2B
- Infrastructure Audit
- Professional Audit
- Software Audit
- Software Down Time

Problems with G2G
- Project Budget
- e-Go v. Frar work

Other Problems

e-Governance Framework

Traditional Audit

Standards

Problem less e-Gov.
5.2 SHORT TERM AND LONG TERM PLANNING

5.2.1 INTRODUCTION

Determining the goals, functions of the e-Governance and the means of achieving these is done in planning phase. Every e-Governance activity commences with planning phase and it is followed by different phases like Organizing, Leading and Controlling. Organizing includes gathering, allocating and coordinating the resources needed by e-Governance applications to accomplish the goals. Leading includes motivating, guiding and communicating with personnel who participate in e-Governance activities. Controlling includes actual performance with planned performance as a basis for taking any corrective actions that are needed.

5.2.2 DEVELOPING PLANNING ACTIVITIES

Top management of concern departments is responsible for preparing a master plan for the e-Governance activities. The plan sets both the long-run and short-run directions. The three important phases of plan preparation are

- Recognizing opportunities and problems of organization by introducing e-Governance applications.
- Identifying the resources needed to for e-Governance activities
- Formulating strategies and tactics for acquiring the needed resources and process.

Auditors should evaluate whether top management has formulated a high-quality information systems plan appropriate to the
needs of the e-Governance applications. Poor planning leads to insufficient hardware, software and personnel resources to handle the e-Governance applications.

5.2.3 TYPES OF PLANS

Top management must prepare two types of information systems plans - strategic plan and operational plan.

A) LONG TERM - STRATEGIC PLAN

The strategic plan is the long-term plan for the next three to five years of operations. The contents of a strategic plan typically include the following

Evaluation of Current applications: Existing e-Governance application services, current hardware/software platform, existing personnel resources, current technology issues, current strengths and weaknesses, current threats and opportunities are to be evaluated.

Direction of planning: Future information services to be provided through e-Governance applications and overall strategies are to be determined.

Development strategy: Vision statement for future e-Governance activities, future applications and databases, future hardware/software platform, future personnel resources required, future financial resources required, approach to monitoring the implementation of the strategy.

B) SHORT TERM - OPERATIONAL PLAN

The operational plan is the short-term plan for next one or two years of operations. The contents of an operational plan typically include the following
Report on progress: The progress report on current plan initiatives achieved and missing are to be prepared timely.

Initiatives to be undertaken: Should observe initiatives to undertake regarding the systems to be developed, hardware/software platform changes, personnel resources acquisition and development, financial resources acquisition for e-Governance activities.

Implementation schedule: Proposed start and finish dates for each e-Governance application, its milestones and project control procedures to be adopted.

Both the strategic plan and the operational plan need to be reviewed regularly and updated as the need arises.

5.2.4 NEED FOR PLANNING

e-Governance planning needs changes from application to application, organization to organization, state to state and country to country. Planning varies depending on type of application. Some operate in unstable environment and auditors should expect these organizations to devote substantial effort in planning. In other organizations, however, the environment is relatively stable.

When auditors evaluate how well top management undertakes information systems planning, they must first determine the nature of and amounts of planning that should be undertaken given their organization's needs.

5.2.5 STEERING COMMITTEE

At most responsibility for e-Governance planning should be vested in e-Governance steering committee. The steering
committee should assume overall responsibility for the activities of e-Governance applications. The e-Governance plan is a critical tool needed by the steering committee to discharge its responsibilities. e-Governance steering committees works best if they have only a small number of members. Their makeup should vary depending on how critical the e-Governance function is.

The steering committee should be chaired by the chief executive officer. Membership should comprise a broad base of senior users and senior information systems personnel. In support organizations, however, extensive senior representation on the steering committee is not so important. Middle-level management representation is likely to be more appropriate.

5.3 AUDIT ON SERVICES

5.3.1 INTRODUCTION

An e-Government service is defined as an application, or series of applications, on the Internet that provides a specific service to a citizen or business. The applications are interactive and transaction based. This means information is collected or provided by the customer and a service is then delivered which completes a transaction. The goal of an e-Service is to provide a start-to-finish solution to the customer. For example, a citizen seeking to pay house tax online, payment is collected and then the e-Governance application delivers the service including all necessary information and documentations like tax payment receipt to the customer. Other online services includes vehicle license, online goods purchasing etc.

Coverage of Critical citizen services is the prime criteria for selection of an e-Governance project for audit.
5.3.2 SERVICES INVOLVED WITH e-GOVERNANCE APPLICATION

The auditors should first sort out the involved services of e-Governance. The various services are designing, developing and implementation of the Internet application, Training on use of services, Marketing of service capabilities, Customer service support, Maintenance of existing services, Collecting and reporting summary statistics on e-Services performance and usage, Electronic payment acceptance related services, Annual surveys of customers/government partners.

5.3.3 e-GOVERNANCE SERVICES DETERMINATION AND IMPLEMENTATION

This addresses two of the e-Governance services audit objectives. The first is Auditors should determine the processes and criteria established to identify, evaluate, and prioritize the development and implementation of e-Services. The second is reviewing the methodologies used to determine the fees that fund e-Services.

The primary decision makers for day-to-day e-Services are Department of Administration (DoA) management, staff and the agency-designated project manager for the e-Service being developed or administered. Additional guidance comes from the Electronic Government Advisory Council. The Council meets quarterly to review reports of e-Services and guide as necessary.

5.3.4 IDENTIFICATION OF NEW e-SERVICES

A process has been established for the development and implementation of an e-Service. First, someone must visualize
an e-Service that fits the contracted work criteria and definition of an e-Service developed by DoA. New e-Services are identified in four ways:

- e-Service successful in another state.
- An agency internally identifies a government service that could be available on the Internet.
- A business or customer base asks for specific services to be provided on the Internet.
- DoA solicits an agency to develop specific e-Services based on industry knowledge and technological capabilities.

5.3.5 PERSPECTIVES OF e-SERVICES

Once there is an idea for an e-service, DoA management, agency designees and others meet to conduct an overview of the project and gather initial information. The idea of e-Service is viewed in the following three perspectives.

CUSTOMER PERSPECTIVE: The first step involves review of the target market by identifying if customers are interested in using this type of e-Service. Additionally, decision makers review if the proposed e-Service will provide added convenience or savings.

AGENCY PERSPECTIVE: This step includes deciding if the agency or the state will gain efficiencies and possibly cost savings by implementing the e-Service. This step is the responsibility of the agency and is not assessed by DoA, but is included in their decision making process.
PORTAL PERSPECTIVE: DoA management determines if the service will bring new users to the portal, which could potentially increase the awareness and use of existing e-Services.

If a project contains all three perspective positively, all parties involved discuss timeframes for development and implementation of the service, agency resources required, electronic payment acceptance terms, conditions, options and fees.

5.3.6 PROJECT PRIORITIZATION

Auditors should look into the process of project prioritization. The demand for online access to government services is growing. As multiple e-Governance applications are to be developed, a development schedule is prepared for those services that have passed the above said three perspectives. Once an e-Service is approved and scheduled, it means everyone involved has agreed to work on the project and dedicate resources as needed. e-Services are listed on the schedule in priority order. Project rankings are determined by evaluating the value of the service and the project resources available. The level of importance in providing the service is defined.

5.3.7 e-SERVICES DEVELOPMENT PROCESS

Auditors should evaluate each and every step involved in development process. The development and implementation process of an e-Service involves the following steps:

- **Staff** meetings are conducted to gain an understanding of internal processes related to the program service and to share design ideas.
• e-Services may be moved ahead of schedule or bumped down the development schedule depending on many factors.
• Development schedule progress and revision decisions are made periodically.
• A pilot project is provided to the agency for review and acceptance.
• Once a service is produced, it is tested for a specific time period and bugs are worked out.
• Training programs are conducted for agency personnel and customers, as needed, on how to use the e-Service.
• The e-Service is then made available to public to make use of it.

5.3.8 e-SERVICES FEES

Auditors should concentrate much on the financial transactions, which is the fee charged by the government for e-Services. There are two types of fees associated with an e-Service.

The first fee is a convenience fee charged by government to pay for the services it provides. For this audit report, a convenience fee is defined as an amount added to a transaction of an e-Service. In general, any e-Service that collects money of any amount has a convenience fee added to it.

The second fee associated with e-Services is a fee charged for acceptance of electronic payment (e-payment). These fees are associated with the method used to pay for e-Service transactions and are termed “cost of sale” fees. There are two e-Payment methods available (credit/debit cards or electronic checks). Fees vary depending on the method used. These fees
are charged by and paid to the credit card network and merchant banks.

5.3.9 AUDITING e-SERVICES SUCCESS

Auditors should measure the success of e-Services as follows.

- The e-Service success is measured by its adoption rate. The adoption rate is the percentage of people using the e-Service versus the total number of people that use a particular traditional government service.
- Other e-Service success factors include revenue generated versus total production and maintenance costs
- Awards or national recognition and citizen or business compliments.

According to DoA management, to ensure the success of an e-Service target markets need to be analyzed, e-Service users need training, e-Service fees should be reasonable and comparable to other service delivery methods, the service needs to be marketed and Performance measures in the form of usage reports are analyzed.

5.4 SOCIAL AUDIT

5.4.1 INTRODUCTION

e-Governance is the process designed for public benefit. Hence while designing the e-Governance applications, it the responsibility of government to make people participate in its design and implementation. In the democratic country, Indian government should focus on the people's problems and perception. The government should share their views and ideas
before implementing the e-Governance applications. In this regard, the social audit plays important role.

A social audit is a process in which the people work with the government to monitor and evaluate the planning and implementation of a scheme or programme, or indeed of a policy or law. The social audit process is critically dependent on the integration and wide distribution of all relevant information. In order to discuss the question “How the social audit is related to other types of audits?”, first we should consider different types of audits in connection to public. They are Government Audit, People’s Audit, Social Audit

**A. GOVERNMENT AUDIT:** This is done usually by professional auditors without significant involvement of affected people. They concentrate on two aspects. Firstly they assess primarily procedural integrity and outputs, Secondly they concentrate on ability to get public perceptions or verify outcome.

**B. PEOPLE’S AUDITS:** This is conducted by the people, sometimes with assistance from NGOs, with a standing invitation to the government. Points to observe are getting public perception, local knowledge and public verification. They can assess outcomes and priorities.

**C. SOCIAL AUDIT:** Conducted in participation of both by the government and the people, especially by those people who are affected or by the intended beneficiaries of the scheme being audited. This can bring the views and facts of the people look at progress. This makes participate the people in the task of verification and the chances of acceptability by the government are high.
5.4.2 SCOPE OF A SOCIAL AUDIT

A social audit is conducted over the life span of a scheme or programme and not just in one stage. It audits planning, implementation, monitoring and evaluation that is it audits the process, the outputs and the outcome. The various elements involved in social audit are as follows.

- Raising awareness of rights, entitlements and obligations under a scheme.
- Specifically, about the right to participate in a social audit.
- Ensuring that all forms and documents are user friendly.
- Ensuring all relevant information is accessible, displayed and read out.
- Ensuring that the decision making process is transparent, participatory and, as far as possible, carried out in the presence of the affected persons.
- Ensuring that all decisions and their rationale are made public as soon as they are made.
- Ensuring that measurements, certification and inspection involve the affected people on a random and rotational basis.
- Ensuring that there are regular public hearings where the scheme and the process of social auditing is publicly analyzed.
- Ensuring that the findings of social audits are immediately acted upon.
- Also ensuring that these findings result in the required systemic changes.
5.4.3 PHASES OF A SOCIAL AUDIT

Social audit is done in three phases. They are as follows

PHASE 1 - PLANNING AND DATA COLLECTION

- Explains the strategic focus of e-Governance applications
- Gather information from households and key informants in a panel of representative communities regarding e-Governance applications, their requirements and utilization
- Proposes and conducts pilot test

PHASE 2 - EVIDENCE-BASED STUDY

- Link household data with information from public services
- Analyze findings in a way that points to action
- Take findings back to the communities for their views about how to improve the situation
- Bring community members into discussion of evidence with service providers of e-Governance

PHASE 3 - PUBLIC ANSWERABILITY

- Conducting workshops of e-Governance applications
- Establishing communication strategy
- Media training to operate e-Governance applications
- Partnerships with civil society in order to enhance/update the e-Governance applications
5.4.4 SEVEN KEY FEATURES OF A SOCIAL AUDIT

i. COLLECTING THE EVIDENCE: Collect data systematically from households, schools and communities, as well as from the service-provider to guide planning and action of e-Governance.

ii. COMMUNITY PARTICIPATION: Communities not only co-produce the data but through involving community representatives, they also help design local and national solutions in development of e-Governance applications.

iii. FAIRNESS: A community-based audit by a neutral third party can help to promote a culture of transparency and strengthen service credibility with fairness.

iv. STAKEHOLDER INVOLVEMENT: All those who have a significant stake in service delivery are actively involved throughout the audit, from the initial design stage right through to implementing community-led solutions.

v. NO ALLEGATIONS: A social audit is intended to focus on systemic flaws and program content, rather than on individuals or organizations. Even negative findings can be framed as a starting point for improvement of e-Governance.

vi. REPEAT AUDITS: Several audit cycles are usually needed to measure impact and progress over time, and to focus planning efforts where they can be most effective.

vii. RESULTS SHARING: A communication strategy, including feedback to communities, mapping and media dissemination is part of every social audit design and especially in social audit for e-Governance applications.
5.5 INFRASTRUCTURE AUDIT

5.5.1 INTRODUCTION

e-Governance projects with transparency and decreasing corruption is catching eye of public. The expenditure or the efforts, invested or likely to invest on the infrastructure creation for the e-Governance application should be considered. Providing information to public at large and complexity of technology used in the e-Governance project should be considered by auditors along with infrastructure requirements.

5.5.2 INFRASTRUCTURE

The infrastructure includes all the physical and abstract elements which are involved in developing and implementing the e-Governance applications. The telecommunication network, electricity, Kiosks, different source of access media like Mobiles telephony, Radios, Computers and Television, security devices like smartcards, biometrics, etc can be considered as infrastructure. As multiple elements are involved in the development of e-Government projects, the infrastructure is habitually the element most open to compromise and this is the one that frequently presents the greatest risk to e-Government projects.

The Office of e-Government, the production Services office, and the Network Infrastructure and Telecommunications office have been given the responsibility to build and maintain the infrastructure. The Office of e-Government and the Office of application development and maintenance Services are responsible for developing web enabled applications and its supporting infrastructure. To build confidence in public and to utilize the e-Governance applications, proper hierarchy and
coordination among infrastructure supervisory departments should be established and it is to be audited.

5.5.3 IDENTIFICATION OF INFRASTRUCTURE

Identifying the infrastructure which is associated with the e-Governance application is difficult because of two reasons. First, the e-Governance application possesses a substantial number of information systems assets. For example, an application may be operated on several micro computers, a wide-area communications network, many local area communication networks, and thousands of files and programs. Second, the e-Governance infrastructure might be widely distributed throughout districts, states and countries and it is not in single location.

5.5.4 CATEGORIES OF INFRASTRUCTURE

One way to identify infrastructure elements is to seek out instances within various general categories as follows.

**HUMAN RESOURCES:** Auditors should consider personnel as the part of infrastructure who is asset of the organizations. The skilled employees, programmers, operators, analysts, end users and others are assets to produce effective e-Governance applications. Hence the auditors should audit for proper personnel. The inexperienced and unskilled personnel may not give good productivity in the e-Governance applications.

**HARDWARE:** The e-Governance applications need adequate hardware than the normal applications. The reason for this is it needs networking communication devices like cable communications, mobile networking, satellite communications, antenna communications to have online interactivity between
government, public and other business communities. Connectors, routers, bridges, boosters and other network related infrastructure are to be taken considered by auditors in their auditing activities. Apart from these, the regular computer systems like minicomputers, main frame systems etc. gets involved in the regular auditing activities.

**FACILITIES:** Unless and until the environment is comfortable, the e-Governance activities cannot be carried forward. The facilities are to be provided for smooth functioning of e-Governance activities. The facilities include proper working space, which is the office environment, the furniture facilitated for the personnel, the computer rooms, tape storage racks and other related things.

**DOCUMENTATION:** Clarity on application or its operational part is obtained though documentation. The documentations are generally ignored and most of auditors will not consider as infrastructure. But the documents are the assets of the organizations which include Systems and program documentation, database documentation, standards, plans, insurance policies, contracts and related items of e-Governance applications which are to be audited.

**SUPPLIES:** The preprinted forms, office stationary, disks, tapes, cassettes are the part of e-Governance infrastructure. The unavailability of these items may cause serious operational problems and hence they are to be audited by the auditors.

**DATA / INFORMATION:** The database, master files, transactional files are the real logical assets of the organization. In e-Governance applications the public data is stored in the database and it is to be protected. All types of security
measures are to be applied on the data which is precious. This is part of e-Governance infrastructure which is to be considered by in auditing activities by auditors.

**APPLICATION SOFTWARE:** The various applications software which are used to maintain the e-Governance activities are to be audited. The software like staff payroll, bill of materials, office maintenance applications, net work maintenance applications, security providing applications and other related applications are to be considered as part of e-Governance infrastructure and they are to be audited.

**SYSTEM SOFTWARE:** System software is the base for any system to operate. It is the part of e-Governance of infrastructure. The Compilers, utilities, operating Systems, communications software others are to be audited for their proper functioning of e-Governance applications.

For every category, review teams are to be appointed and it is their duty to prepare a comprehensive list of assets. The infrastructure identification becomes costly, for the finer level of asset identification.

**5.5.5 VALUATION OF INFRASTRUCTURE**

Valuing the infrastructure is difficult task because of the following points

- The valuation might differ from place to place, person to person and depending on situation.
- The valuation also depends on the way in which the infrastructure could be lost, the period of time for which it is lost, and the age of the infrastructure.
- The other point to be considered is it depends on the time line of e-Governance application.
- In most of situations the valuation of physical infrastructure cannot be done in isolation from valuation of logical infrastructure. For example the cost of physical hard disk or tapes may be less but the data it contains may be very expensive.

Keeping the above points in view, the auditors should use their skills in valuation of infrastructure.

5.5.6 SAFE GUARDING THE INFRASTRUCTURE

The e-Governance auditors should sense the major security threats for infrastructure. They should safeguard them with different auditing techniques. Auditors must understand the nature and potential consequences of threat for infrastructure and take remedial measures through concern security authorities. Some of the points to be considered in safe guarding the e-Governance infrastructure are as follows

**HUMAN RESOURCE:** Human resource is the back bone for any organization. Training and constant updating the staff in all regards is required to maintain the staff. Assigning the duties of one staff to another periodically will make any staff to take up the work of any other staff. This helps in tuff times when staffing problem occurs. Auditors should even see that backup staff is maintained or arrangements with another company were made, if the present staff creates problems.

**HARDWARE:** Back up hardware should be maintained to sustain the problems and for immediate hardware failure recovery. Auditors should also see that necessary arrangements are done with other companies to share their hardware in trouble some situations.
FACILITIES: Caution should be taken by auditors to prevent structural damages, furniture damage and other disturbance for facilities. Proper arrangements should be taken with other organizations to have backup facilities in crisis.

DOCUMENTATION AND SUPPLIES: Auditors should see that the e-Governance documents and supplies are stored securely on site. If any disaster occurs, then to be on safe side they are to be stored off site.

DATA AND SOFTWARE: Auditors should see that the data backup, application and system software should be maintained on site and off site to avoid calamity.

5.6 PROFESSIONAL AUDIT

5.6.1 INTRODUCTION

Professional audit is one of the key points in e-Governance framework. As per this the skills of various IT professional are audited to see whether they obey certain standards to fit into the work to produce quality E-Governance applications. As most of the e-Governance applications are online, and many of the citizens, organizations and others interact with these applications, the professionals who develop these applications should possess certain qualities to receive the appreciations. If not appreciations, the applications should not cause any damage or inconvenience to public or organizations. The e-Governance applications are basically brain work and hence they are to be audited.

5.6.2 PROFESSIONALS TO AUDIT

Every organization needs staff that is competent and trustworthy. Extensive power is often given to the persons responsible for the computer based information systems.
development, implementation, operating, and maintaining within organizations. Unfortunately, ensuring that an organization has competent and trustworthy information systems personnel is a difficult task. Some information systems personnel seem to lack a well-developed sense of ethics and some lacks technical skills. In connection the IT professionals working for e-Governance applications should be audited regarding their trustworthiness and their skills. The various IT professionals whose duties to be audited are as follows

- **SYSTEM ANALYST**: Analyst gathers the information requirements for the projects to be developed by analyzing the problem and gives design to solve the problem. The information system architecture for the e-Governance or any other related projects should be given by him.

- **APPLICATION PROGRAMMER**: He is responsible for designing programs to meet information requirements. He develops codes, tests, and debugs programs. He should also develop help documents for the programs designed. Sometimes he needs to modify programs to rectify errors or to improve the performance of the program.

- **SYSTEMS PROGRAMMER**: He should maintain and enhance operating systems software, network software, library software, and utility software which help for e-Governance applications. He should also take care of various system abnormalities.

- **DATA ADMINISTRATOR**: He should gather the data requirements of the users of information systems services of e-Governance applications. He designs policies for data and should maintain perfect documentation for data.
• DATABASE ADMINISTRATOR: He is responsible for the operational efficiency of databases. He should also maintain access control over the database and assists users to use databases better.

• SECURITY ADMINISTRATOR: He implements and maintains physical and logical security over the information systems function. He monitors the status of security over the information systems function. He should also investigates security breaches.

• NETWORK ADMINISTRATOR: He is responsible for proper functioning of networking systems. The e-Governance applications which are designed to work on local area networks, wide area networks, internet and intranets should be free from network problems. These problems are rectified under guidance of network administrators.

• WORKSTATION SPECIALIST: He should advise on the selection, implementation, operation, and maintenance of different types of workstations. The data entry workstations, end-user workstations and designing workstations are his prime duties.

• CLIENT SUPPORT SPECIALIST: He advises end users on analysis, design, and implementation of systems. He determines needs for end-user tools; supports use of end-user tools.

• QUALITY ASSURANCE SPECIALIST: He should establish quality control standards for the information systems function. He ensures all systems conform to quality assurance requirements before they are released into production.

• DECISION SUPPORT SYSTEM SPECIALIST: He should gather requirements and designs and builds executive information
systems and decision support systems. He should undertake corporate modeling, determine needs for new executive support and decision support tools.

- **EXPERT SYSTEM SPECIALIST:** He should gather requirements, design, build, and maintain expert systems. He should also document expert systems and should determines need for new expert-system tools.

- **OPERATIONS SPECIALIST:** He plans and controls day-to-day operations, monitors and improves operational efficiency and assists with capacity planning.

- **COMPUTER OPERATOR:** He is responsible for maintaining and operating the computer and related equipment.

- **LIBRARIAN:** He should maintain library of magnetic media and documentation.

- **DATA ENTRY OPERATOR:** He prepares and enters data at workstations or terminals.

- **SUPPORTING CLERK:** He maintains and operates transfer pricing system. He acquires consumables needed by the information systems function. He registers and follows up on user complaints. He maintains information systems accounting systems, handles user inquiries, collates and distributes reports.

### 5.6.4 FACTORS TO CONSIDER

**SEPARATION OF DUTIES:** While auditing the professionals the two important points to be noticed are see that all the professionals are very clear with their roles of duties in e-Governance applications. The duties of one professional should
not interfere with the duties of other professional. That is there should be separation of duties. While auditing one should see that the hierarchy of the designations is proper. The placement of the information system department in the organizational hierarchy is important. Improper placements will lead to inconvenience, misunderstanding and firing among the professional. This hampers the smooth functioning of information department.

**CHANGE MANAGEMENT - CHANGE IN MANAGEMENT:** If it is noticed that there is inefficient and unskilled staff, then it is better to replace them with skilled one. This is called as ‘change management’. Sometime, the staff may be efficient and skilled but the management may be with inefficient managerial skills. In such cases, the major deciding factor is ‘change in management’. That is the existing management should be changed with new skilled qualified management. The second case is a difficult task because it is the deal with the higher officials.

**ENCOURAGEMENT:** There are various strategies for motivating professionals. The strategies change from person to person depending on characteristics of individuals and the on the surroundings of working environment. Some gets motivated with words, where words makes magic. Some gets motivated with promotions and some with perks and so on. Before motivating the professionals, the parameters to be considered are statistics on staff turnover, their failures, success, their regularity and their attitude.

**QUALITIES OF PROFESSIONALS:** While auditing professionals, certain qualities are to be examined by the information system auditor. These qualities will help to develop the e-Governance applications to develop with quality and within the time span.
The qualities are Consciousness, Empathy, Self control, Predictability.

**STAFF RELATIONS:** Relations among the staff member should be very strong and their communications should be effective. This is very critical factor between top management and subordinate staff. Relations and communication among staff will make the organization to plan, organize and develop the best e-Governance projects by creating strong bondage among the staff and oneness.

Auditors should observe the communication channels and see that the overhead transmissions are not taken place. The auditors should adopt both formal and informal strategies to enhance the effectiveness of communication among the IT professionals.

**STREAM LINING THE DUTIES:** Sometimes the staff will be sincerely discharging their duties but with some deviations. While auditing the professional deviations are to be stream lined and see that the work is on track. Neglecting the small deviations in work may pay big dividends in the latter stages. At every stage of developing e-Governance applications, the planned activities should be compared with the ongoing activities and diversions are to be rectified.

**STUDY OF STANDARDS:** The auditors should see that the information system professionals obey certain standards while working with e-Governance applications. The standards are Procedural values, Performance values, Recording values, Project-control values.

**STAFFING CONCEPTS:** Auditors should concentrate on three areas in staffing which includes recruiting the professionals for e-
Governance applications, developing the professionals and terminating the professionals.

CODE OF CONDUCT: Auditors should see that code of conduct is designed and strictly implemented in order prevent misuse of software, data, and services. The code of conduct should govern the actions of information systems. This is one of the important areas related to the behavior of professionals. As the most confidential data of the public and organizations are with the e-Governance application development professions, action to be taken who miss utilizes it.

IMPROVING PROFESSIONAL SKILLS FOR E-GOVERNANCE

Professional skill is typically identified as having three components: knowledge, skills and attitudes. The Experience of auditors can play a lead role in both analysis and training the professionals. Beyond this generic activity, a number of more specific proposals can be made about building competencies for e-Governance:

TRAINING PROGRAMS: Training content should contain appropriate topics which are applicable for regular discharge of duties, used to integrate various e-Governance that helps to adapt solutions for various real time problems and the need for better communication with important clients or customers. e-Governance hybrids closes the gap between IT professionals, civil servants and politicians. Training should also concentrate to Bridging gap between genders, change of attitude. The training programs can be conducted online, offline, in-house training, out-house training and distance training program. Preparing local IT Industry for e-Governance applications, will aid in including local languages and in solving local problems. The alternative modes of training
includes Teacher-centered model, learning diaries, learning from groups of staff from different organizations sharing learning experiences, work shadowing, job exchanges, attending seminars, attending exhibitions, reading journals and magazines.

5.6.5 SKILLS AND KNOWLEDGE REQUIREMENT FOR e-GOVERNANCE PROJECTS

SYSTEMS DEVELOPMENT CAPACITY: Instead of depending on hired or foreign programmers, the native information systems development capacity for e-Governance must be strengthened, both within user organizations in the government and NGO sectors, and within private sector vendor organizations.

PROJECT/CHANGE MANAGEMENT CAPACITY: The public sector particularly has been poor at managing e-Governance projects and at managing change. That capacity needs to be strengthened.

INTELLIGENT CUSTOMER CAPACITY: Public sector organizations especially have been poor ICT customers, unable to raise the finance for projects, unable to specify their needs, unable to manage the procurement process, and unable to manage vendors. All of these capacities need to be addressed to change a client-vendor relationship.

OPERATIONAL CAPACITY: Finally, the ability of the public sector and other governance-related organizations to operate and maintain information systems must also be strengthened. For almost all developing countries this will still initially include a need to build basic computer literacy skills within user communities.
5.7 SOFTWARE AUDIT

5.7.1 INTRODUCTION

The software which is used for the e-Governance applications should be audited for correctness, perfectness and availability. The software audit comprises Application software audit, Database audit and System software audit. In Application software audit, programs which are developed for e-Governance applications, the purchased programs, network protocols, the related packages and utilities are to be audited by auditors. In Database audit, the data which is acquired through application programs are stored in database and audited. In System software audit, the operating system, firmware, hardware that permits sharing and resources within a computer system are audited.

5.7.2 APPLICATION SOFTWARE AUDIT

Application software audit in connection to e-Governance should mainly cover the business rules in the flow and accuracy in processing, Validations of various data inputs, Logical access control and authorization and Exception handling. The various auditing elements are as follows.

REVIEW OF DOCUMENTS: Study and review of documentation relating to the application. However, the IS auditor may find situations in real life where documentation is not available or is not updated. In such cases, the auditor should obtain technical information about the design and architecture of the system through interviews.

FUNCTIONS OF SOFTWARE: Study key functions of the software at work by observing and interacting with operating personnel during work. This gives an opportunity to see how processes
actually flow and also observe associated manual activities that could act as complementary controls.

EXECUTE THE PROGRAM OPTIONS: Go through the menu items, features and options to identify processes and options for conformance to business rules and practices. This kind of run-through can be done more effectively if a development/test system is made available to the IS auditor. In the absence of such a facility, the auditor only can watch the system run by the system administrator and make notes. The auditor is advised not to do any testing on a e-Governance production system as this could affect adversely a "live" system and public gets effected.

VALIDATIONS: Validate all the inputs of the system against different conditions. Such validations go a long way in eliminating errors and ensuring data integrity. Apart from simple validations for numeric, character and date fields, all inputs should be validated with range checks, permissible values, etc. Validation checks that are built on application-specific logic can act as powerful controls not only for ensuring data accuracy but also to prevent undesirable data manipulations. The IS auditor can check validations by actually testing them out in the development/test system.

ACCESS CONTROLS: Access control mechanisms of application software should be verified. There are two point to be considered related to access control are the design of the access control module and the nature of access granted to various users and its maintenance.

The design of the access control module may be of varied types. Most software would check a combination of user id and passwords before allowing access. Access may be controlled for
each module, menu option, each screen or controlled through objects. The IS auditor should review the design of the access control module keeping in mind the criticality of the functions possible in the software and evaluate whether the design provides the level of control and granularity to selectively and strictly allows access as per the job requirements of all the users. The auditor should proceed to verify whether all existing users have appropriate access as evidenced by their job descriptions and whether access to certain critical activities are allowed only to select personnel duly authorized. It also is necessary to verify who has administrator / super user rights and how such rights are used /controlled.

**EXCEPTIONS:** Verify how errors and exceptions are handled. In many activities software provides options and ways to reverse transactions, correct errors, allow transactions under special circumstances etc. Each one of these is special to the business and based on the rules and procedures defined by the e-Governance. The IS auditor needs to see how the software handles these.

**CORRECTIONS:** Correct any weaknesses found at the end of an applications review in the software that could lead to errors or compromises in security. These would need to be corrected by either changes in design or some recoding. While this would be addressed by the IT department, the user or owner of the application from the functional area would want to know if any of these weaknesses have been exploited by anyone and whether there have been any losses. To provide an answer to this question the IS auditor should download all the data for the period in question and run a series of comprehensive tests using an audit software and determine if any error or fraud really occurred or not.
REVIEW OF RELATED SOFTWARE: Evaluate the e-Governance environment under which the application runs. The audit of the application software alone is not enough. Generally, it is prudent to conduct a security review of the operating system and the database in which the application runs while doing an application review.

The job of application review becomes more complex as the application becomes larger and integrated.

5.7.3 DATABASE AUDIT

The database subsystem is responsible for defining, creating, modifying, deleting, and reading data of e-Governance applications. It maintains declarative data, relating to the static aspects of real-world objects and their associations, and procedural data, relating to the dynamic aspects of real-world objects and their associations.

ACCESS CONTROLS: Access controls used in the database subsystem to prevent unauthorized access to and use of data are to be audited. A discretionary access control policy can be used, which allows users to specify who can access the data they own and what action privileges they have with respect to the data. A mandatory access control policy requires a system administrator to assign security aspects to data that cannot be changed by database users.

INTEGRITY CONSTRAINTS: Auditors should verify various types of integrity constraints to maintain the accuracy, completeness and uniqueness of instances of the constructs used within the data modeling.
CONCURRENCY CONTROLS: Auditors should take care of concurrency controls in a distributed database environment. They can be complex. In a replicated database, one solution to the concurrency problem is to designate one replica of the database as the primary copy. Before accessing a data item, a transaction must acquire the lock for the primary copy. In a partitioned database, a transaction must first find the scheduler for the data item it is seeking to access.

CRYPTOGRAPHIC CONTROLS: Auditors should verify the various cryptographic controls that are used to protect the integrity of data in the database. To protect one user's data from access by another user, cryptographic keys must be assigned to the owner of the data and those users who are allowed accessing the data.

FILE HANDLING CONTROLS: File handling controls are to be observed by auditors which are used to prevent accidental destruction of data contained on a storage medium by an operator, user, or program. They include internal labels, generation numbers, retention dates, control totals, magnetic tape file protection rings, read-only switches, and external labels.

AUDIT TRAILS: The accounting audit trail in the database subsystem should see the maintenance of the chronology of events that occur to the database. The operations audit trail in the database subsystem maintains the chronology of resource consumption events that affect the database.

BACKUP: Auditors should see the backup arrangements are perfect. The grandfather, father, son backup, the dual recording or mirroring backup, the dumping concepts and the logs are to be checked.
RECOVERY: Auditors should verify the controls that are needed to recover the database from types of failure.

5.7.4 SYSTEM SOFTWARE AUDIT

Auditors should consider the following points regarding system software audit.

PROTECTION FROM USER PROCESSES: Auditors should see that the operating system must be protected from user processes. A user process must not be able to bring a computer system to a halt, destroy essential information, take control of the system, or change the system in an unauthorized way.

MUTUAL USER PROTECTION: Auditors must assure that the system software should not disturb the users processes. Users must be protected from each other. The operating system must prevent one user corrupting another user's processes or data.

USER PROTECTION: Users must be protected from themselves. A user process might comprise several distinct modules or sub-processes, each with its own memory area and files. One module or sub-process should not be able to corrupt another module or sub-process.

SELF PROTECTION: The operating system must be protected from itself. One module or sub-process in the operating system should not corrupt another module or sub-process.

ENVIRONMENTAL PROTECTION: When environmental failures occur, the operating system should be robust. For example, if a power failure occurs the operating system should be able to bring operations to an orderly halt.
INTEGRITY THREATS: Threats to operating system integrity can be accidental or deliberate. Accidental threats include hardware, software, and environmental failures that cause the operating system to crash or to process erroneously. Deliberate threats to operating system integrity usually aim at unauthorized removal of files, breaches of data integrity or disruption of operations. These threats are to be predicted by the auditors and remedial measure is to be taken.

INTEGRITY FLAWS: Operating system penetrations result when integrity flaws exist in operating systems. These flaws arise for two reasons. First, the access control policy designed for the operating system is defective. Second, even if a secure access control policy is designed for the operating system, it might be implemented incorrectly in the operating system. These issues are to be audited by the auditors.

DESIGN CONSIDERATIONS OF OS: Because an operating system is complex, critical software, auditors should be concerned about the approach used to design and implement it. The top-down design, structured programming principles are preferred in designing the operating system. In the layered approach, auditors can have more confidence in its reliability.

OS CERTIFICATION: In an effort to improve operating system integrity, government has developed criteria that only certified operating systems should be used in developing e-Governance applications and it is to be audited by Information System Auditors.

5.8 DOWN TIME AUDIT

5.8.1 INTRODUCTION

Performance audit reports concern the efficiency, effectiveness, economy of a particular government activity.
The performance is directly related to downtime of e-Governance application. The measure of e-Governance performance is the citizen satisfaction in terms of convenience, increased transparency and protection of the confidentiality, integrity and the reliability of the information stored and processed by the e-Governance applications.

5.8.2 DOWNTIME TROUBLES

In e-Governance applications, the software and networking plays important role in exhibiting the performance of e-Governance application. As networks have grown in speed and ubiquity, their complexity has grown quickly. e-Governance applications make use of desktop computers, servers, LANs, WANs and the Internet. Hence the probability of network downtime is more. There are 2 types of network service interruptions leading to breakdown of e-services. First is degradation, when a service is slower than usual and the low performance services perhaps may be useless which lead to outage. The second is a customer accessing a Web site may be unavailable.

Auditors should probe enquiry into such problems. They should see that network management tools are properly used and IT qualified staff are appointed. Even then the downtime still happens, and the costs can be shocking.

5.8.3 SOURCE OF DOWNTIME

The different sources of downtime identified are Network, Security, Cables and connectors, Servers, Applications, Service providers etc. Each of these concepts is involved with
some common causes like Hardware problems, Software problems, Human error and Service provider errors.

**NETWORK PRODUCTS:** Downtime costs associated with network hardware are significant, but not the most troubling area. Network products account for 15% of downtime hours and 17% of downtime cost. Significantly more of the downtime hours associated with network hardware come from service degradations. Seventy-six percent of outage hours associated with network products are caused by hardware or software problems as opposed to human error.

**SECURITY PRODUCTS:** Security products are not a serious source of downtime. Only 7% of downtime hours and 9% of downtime costs can be traced back to security products. Both hours and costs associated with security product downtime are evenly split between outages and degradations. Only 17% of outage hours associated with security products are a result of human error, hardware or software failure are significantly more common.

**CABLES AND CONNECTORS:** Cables and connectors are only a minor irritation when it comes to downtime. They only account for 7% of downtime hours and 5% of costs, most of which is due to largely unavoidable natural disturbances.

**SERVERS:** Servers are very similar to network products in their impact on downtime overall, accounting for 17% of downtime hours and 16% of cost. Downtime hours are fairly evenly split between outages and degradations. Again, human error is not a major factor in server downtime, accounting for only 17% of server outage time.
APPLICATIONS: Application downtime is the largest single contributor to downtime hours (30%) and cost (32%). Application outage cost is more than double the cost of any other downtime source. Human error plays a much larger part in application downtime than in any other area; human error is responsible for 35% of outage time and 39% of service degradation time.

SERVICE PROVIDERS: Service provider problems are the source of 21% of downtime hours and cost. Cost associated with outages and service degradations associated with service providers are roughly equal.

e-COMMERCE: e-Commerce is not a major factor in downtime costs. As many large companies do not offer e-Commerce, and those who do have a good handle on how to keep their commerce sites up and running. e-Commerce accounts for less than 1% of downtime hours and almost no cost.
5.8.4 DOWNTIME ESTIMATIONS

Downtime leads to loss to revenue and productivity loss. Hence there should be some means of estimating the revenue loss and productivity loss incurred due to downtime.

REVENUE LOSS ESTIMATION: As e-Governance applications generate revenue, downtime impacts treasury. We may not calculate the downtime effects exactly but by applying some reasonable assumptions, we can derive a good estimate that can be used to justify the expense and effort involved in avoiding downtime. The use of software products which can identify the problem or even better software products which will identify a potential problem can help to reduce or completely avoid downtime. The points to considered in revenue loss calculation is Total hours of service degradation per year. Total number of revenue Generating employees affected by outages or service degradations. Average percent of productivity lost by revenue Generating employees during degradations. Average annual
revenue generated by each revenue-generating employee. Total
downtime for e-Commerce systems multiplied by average hourly
ecommerce Revenue.

A. PRODUCTIVITY LOSS ESTIMATION: When users are unable to
access network resources their productivity decreases, which
has a distinct impact on a bottom line of e-Services. Large e-
services invest tens and hundreds of millions of dollars in
technologies that increase productivity. In productivity loss
calculation, we use four key pieces of information

- Total outage hours per year and service degradations
due to each of the sources of downtime
- Total number of employees affected by outage or
service degradations
- Weighted average hourly wage per employee
- Average percent of productivity lost by employees
during outages and service degradations

The productivity loss is calculated in terms of revenue
generating employees and non revenue generating employees.

To find productivity lost by revenue-Generating employees

- Multiply the weighted hourly wage per employee by
the number of revenue generating employees affected
by outages or degradations
- Multiply the result by the percent of productivity
lost by revenue-Generating employees during outages
or degradation
- Finally, multiply the result by number of annual
hours of outages or degradations
- To find productivity lost by non-revenue-Generating
employees
• Multiply the weighted hourly wage per employee by the number of non-revenue generating employees affected by outages or degradations
• Multiply the result by the percent of productivity lost by non-revenue-Generating employees during outages or degradations
• Finally, multiply the result by number of annual hours of outages or degradations
• To find total cost of productivity loss by all employees, sum the obtained values.

Down time is a serious problem which causes great revenue loss and hence vigilance it throughout e-Governance applications.

5.9 BUDGETING THE e-GOVERNANCE PROJECT

5.9.1 INTRODUCTION

Most of the countries are opting for e-Governance but there is no pre defined existing budgeting methods. As this is recent concept, budgeting frameworks are not well developed. The definition of e-Governance differs from country to country. Some considers it as departmental implementation, some as the local area implementations and some as national implementation. Hence deciding the budget is complicated issue. The estimation of expenditure and comparison of the costs versus the benefits of e-Government is to be established. The estimation of expenditure differs from one application to another application because of the differing installed bases, capital replacement costs and spending requirements on infrastructures for e-Government readiness. As e-Governance is an online activity, the cost incurred for privacy and security should also be considered.
5.9.3 FUNDING ISSUES AND OVERCOMES

The various funding issues are as follows

A. COST OVERRUNS DUE TO MISS PLANNING OF PROJECTS: For most of e-Governance projects, cost estimates are not up to the expectations and most of the times, cost exceeds the planned cost. A research conducted by "Standish Group" has found that 30% of projects are failures, 45% experience some significant problems and 25% are near to the expectation. Most of the large projects are under performance. The projects which take long duration for developments are with poor cost estimation and generally exceeds its original cost by 30%. This may be because of the hike in resource prices, man power, taxation etc. Poor project planning and ensuing cost overruns are therefore a common problem of e-Governance projects.

From a cost-saving perspective, a convincing argument can be made to governments that they should refocus their strategies on timely cost calculation depending on control, performance and efficient use of human capital. The adoption of such practices also promotes a higher level of transparency in governmental operations.

B. IMBALANCED COST AND SAVINGS: In most of the e-Governance projects cannot predict when the savings will meet the cost. Sometimes, the questions arise; will the cost of e-Government projects is dominating the savings? When can the savings meet the cost? What is its time line? Cost benefit analysis will therefore become a relevant issue in the effort to align information technology with the business of government.

Unlike the private sector governed solely by profit motives, the public sector has a duty to provide public service to its citizens. Hence the government should even consider the public
interest, instead of calculating the cost versus savings. In order to cut down the project costs, government can give the applications as Outsourcing to private parties. However, it needs to be managed properly for cost reductions. Other cost reduction mechanisms include the avoidance of emerging technologies whose incorporation may degrade the performance of the project.

C. MINIMIZING TRANSACTION COSTS AND CORRUPTION IN GOVERNMENT PROCUREMENT: Investments in electronic procurement systems are bound to streamline the procurement process, reducing transaction costs and helping to weed out corruption. Negotiating and concluding transactions through a single unified system is more efficient than other methods. The state's transaction cost has reduced by more than 50% by e-Governance implementations. The greater efficiency and reliability is attained by electronic system transactions, thus shortening the time of transaction. On line discussions between buyers and sellers can be recorded and made publicly available. This mechanism eliminates bribes and other fraud activities among sellers and buyers. The system uses a reverse auction process, with companies submitting bids online and the contract awarded to the lowest bidder. This gives transparent mechanism and the government can get cost benefit out of it.

D. GOVERNMENTAL FUNDING STRUCTURE CONSIDERATION: e-Governance project implementations are dependent on governmental policies and funding structure. Some countries have decentralized government structures and some are with integrated structure. The local activities may force the central government to go for integrated e-Governance implementations. In this case the local budget becomes base to calculate the integrated budget. Some adopt day to day e-Governmental activities; in this case
the budget balancing should be done on day-to-day basis. In order to deal with the budget problems some times, the e-Governance projects are implemented with public and private sector partnerships. By doing so, the private sector’s perceptions will be on revenue generations, implementation of projects and the government sector will concentrate on the public benefits and related aspects. This also helps in sharing the financial matters. Successful e-Governance not only involves technological and funding issues, but also organizational issues. An incremental funding approach might be more appropriate and more likely to be successful.

5.9.4 e-GOVERNANCE FUNDING STRATEGIES

It is identified by government and public that the best service delivery channel is internet. Public expects the best services, faster services and quality services through e-Governance projects. The public expectations are so high with government projects, that they should be better or even more competitive to private sector implementations. Hence there is more pressure on government in pumping the financial facilities to e-Governance projects.

Heavy investment is required in the initial stages e-Government projects which are the direct expenditure. Successful e-Governance may require that governments treat e-Governance projects as capital expenditures. Long term funding arrangements are to be done with arrangements like bonds, leasing arrangements that guarantee long-term funding and smooth expenditures for large investments by spreading expenses over several periods.

CONSIDERABLE ASPECTS FOR FUNDING THE PROJECTS: Government need to evaluate e-Governance projects by following aspects while funding.
• Undertaking a traditional cost benefit analysis and discounting to present value
• Focusing on the underlying cost effectiveness of the project in terms of the ability to produce outputs more effectively than existing arrangements
• Evaluate whether the project constitutes a fundamental building block for long term development
• Focus on how important the need for the project is in terms of ensuring access for all
• Consider the project not only in financial terms, but also in terms of social outcomes and social benefits.

5.9.5 DIFFERENT FUNDING METHODS

ISSUING BONDS: Bond-financing is cheaper than bank loans. This can be done by government, private sectors in tie up with government bodies. Bonds can be issued, on either the domestic or international capital markets. This mechanism of financing allows them to obtain all the funds they need to start the projects and are not subject to partial repayments, as in the case of bank loans. Issuing bonds also allows for longer maturity debt than bank loans. Longer maturity debt helps to minimize the budget risk and contributes to the financial stability. In various countries the different types of bonds issued to private parties to invest in e-Governance which are General Obligation Bonds, Project Revenue Bonds, Dedicated Revenue Bonds, GDP-linked bonds etc.

Instead of the public sector flooding all of its investments in e-Governance projects and to suffer with treasury problems, it is better idea to have a partnership with private sector in funding activities. This is appreciable not only for the funding sake but also to gain the positive aspects of the
private sector which are skilled manpower preparation and recruiting them, enhancing the efficiency of service delivery, preventing from the political intervention and for smooth functioning of activities, takes responsibility to answer and cater the public needs.

Many countries are adopting Public Private Partnerships (PPPs) to fund projects. Private Finance Initiatives (PFIs) which are exclusively funded by private capital, are now the most successful version of public-private partnerships. A typical PFI project is a tightly drafted contract between a government and a private consortium running for 25 to 30 years. Private Finance Initiatives nevertheless, do offer the prospect of refinancing these projects in the capital markets. Refinancing projects makes full sense both for the government and the private share holders.

5.9.6 Inventive Financing Methods

Low Hardware Cost: The government policies of reducing the taxes on hardware and its components resulted in reduced hardware cost. Even the liberalization and globalization policies of government made to start various electronic industries across world. This made the hardware prices come down to rock bottom level. This gave the public as well as private sector to invest in e-Government projects.

Outsourcing: This is another way of reducing the investment on e-Governance projects as the outsourcing companies not only undertake the existing systems, they also offer to install new systems.

Software Leasing: The IT financing market is bursting with increasingly attractive leasing packages. Software leasing is simply the business of choosing to finance the use of software
over an agreed period of time and then having the option of buying the software license (or licenses) at a predetermined price at the end of that period.

RENT TO OWN: Some countries introduced this method which allows users to make use of software for certain period of time by paying monthly rent. If the user uses it for certain period of time, then the user can own that software. If they are not interested to own it then they can quit the deal by giving the prior notice and by paying some cancellation fee.

3-ZERO FINANCING (TRIPLE ZERO): Zero down, zero payments and zero interest - for all new software, hardware and services contracts are announced by some reputed companies. e-Governance projects can make use of these facilities to lower the investments.

5.9.7 RETURN ON INVESTMENT

The return on investment is important factor to be considered in e-Governance. Unless and until the invested funds are returned, the new e-Governance activities cannot be undertaken. Even considering the government as a business organization, it should also aim at profits out of its investments. Some of the return on investment methods is as follows.

GOVERNMENTAL AGENCIES: Innovative new financing methods have been emerging in the Indian governmental sector, where governmental agencies have been shifting the financial burden to vendors by letting them share in the revenue generated through new IT systems.

GOVERNMENT DEPARTMENTS: Ministry of foreign affairs, the passport issuing office, police and criminal justice system are servicing the citizens of India in faster and better way. They enabling citizens to now receive a passport in faster
way, get on line justice in their cases. As there is comfort, the citizens use the online services. The revenue generated for the government is shooting up day by day. The government is offering a percentage of the revenues that accrued to the agencies. This reduces the maintenance burden on government and increases the government revenue.

SHARE-IN-REVENUE: Share-in-Revenue or Share-in-Savings made agencies to participate actively in promoting the online public transactions.

USER CHARGES: As online services are better than off line services, to have economic efficiency considerations and with political fairness the government introduced user charges. The service charge is collected from the users which increases the revenue of government.

ADVERTISING: Around 23% of revenue is generated by online advertisements in the governmental web sites. As most of the public interacts with online web sites, it promotes the business activities of the advertiser which is the source of return on investment.

EXCISE, ENTERTAINMENT AND LUXURY TAX: The various departments started their activities, advertisements online and increasing the public transactions and trade which is generating income in the form of taxes. The first highest revenue is collected by Trade and Taxation department. The Excise, Entertainment and Luxury Tax department is the second highest revenue (Rs. 1950 crores in 2008) collecting department of the Govt. of NCT of Delhi.

5.9.8 FURTHER DEVELOPMENTS FOR RETURN ON INVESTMENT

The Department aims to improve performance by strengthening the distribution network of liquor, widening the tax network and taking effective enforcement action. Some of the major
schemes of the department under 10th five year plan are Automation of Excise, Entertainment & Luxury Taxes Department and strengthening them, establishing excise Control Laboratory. As part of improvement in the activities, different sections of the departments are automated and fully automation is in progress. Some of them are Administration, Litigation, Permits, Accounts, Vigilance, Care Taking, Hotel Club & Restaurant, Luxury Tax, Excise Intelligence Bureau, Control lab, Country Liquor, Entertainment Tax etc. The various steps under implementation for return on investments are as follows

- Computerization of VAT should ensure that the VAT rule is implemented and administered in a manner that achieves the policy objectives of the government.
- Increase the Tax payers base by securing the more reliable source of revenue through computerization. This will increase the efficiency in the collection of tax by streamlining the process of online return filing.
- Effective utilization of resources which can be achieved by having an Integrated Information System
- The computerization of trade and taxation system boosts up the revenue.
- The critical modules of sales tax applications are to be fully computerized which includes Dealer Information System, Tax Accounting System, Return Processing System, Forms Control System, Resource and Inventory System etc.

5.10 STANDARDS

5.10.1 INTRODUCTION

A standard is defined as a technical specification or other document available to the public, drawn up with the
cooperation and consensus or general approval of all interests affected by it, based on the consolidated results of science, technology and experience, aimed at the promotion of optimum community benefits and approved by a body recognized at the national, regional or international level.

Quality of software is the major considerable factor in e-Governance activities. The quality is maintained by following certain global standards which play an important role in building the architecture of e-Governance.

5.10.2 AIM OF STANDARDIZATION

- To make requirements and specifications available in the public domain
- To ensure smooth flow of information between citizen, business and Governments
- To protect consumer interests by facilitating adequate and consistent quality of information and services with human centric design of system
- To promote reduction of effort
- To provide users a common terminology and a framework for communicating technologies across different domains

5.10.3 TYPES OF STANDARDS

The different types of standards are Policies, Technical standards, recommended best practices and Guidelines.

- **POLICIES**: The documents that enforces certain set of instructions that should be mandated in an organization. They usually represent the standards for e-Governance applications.

- **TECHNICAL STANDARDS**: Documents that establish engineering and technical requirements for processes, practices and
methods. They contain the provisions necessary to verify compliances.

- **RECOMMENDED BEST PRACTICES**: Documents that contain authorization, engineering, technical information including architecture, framework and data relating to processes, procedures, practices and methods.

- **GUIDELINES**: Documents that contain technical information in support of specifications and recommended best practices. Guidelines suggest alternative approach to good practice but generally refrain from clear-cut recommendations.

Important documents needed by e-Governance projects are technical standards. They in turn comprises the aspects like Information Access, Presentation, Process, Data integration and Interchange, Metadata, Network Security, Communication Gateway and Data Preservation which are classified under Data and Meta data standards, Security standards, Localization standards and Quality standards.

\[ TYPE \ OF \ STANDARDS \]

Out of various software engineering standards, the dominating standards are Six Sigma, CMMI and BIS. The standards proposed by Indian government for e-Governance projects as per Indian environment are Bureau of Indian Standards (BIS).
5.10.4 SIX-SIGMA

Six-Sigma is a metric of Capability and Performance. Higher the Sigma Level, the better is the performance. At Six Sigma, the process or product meets customer's requirements 99.99966% of the time. This defines a process improvement approach that is based on statistical measurement, drives quality improvement, and reduces operational costs. It helps in developing detailed work instructions and it defines a methodology for continually mapping, measuring and improving the quality process. Six-Sigma can help to determine, how an IT organization manages its services in order to increase the quality of IT delivery processes. A typical well-managed process is supposed to operate at 3 sigma or 93.2% performance. 6 Sigma is a Methodology to revolutionary results which improve processes & products in comparison with conventional evolutionary continuous improvement techniques. Most of the tools and techniques of Six Sigma are quantitative or statistical in nature, while others provide a logical approach to problem solving. Hence Six Sigma works best where Business objectives or Customer requirements are quantifiable & measurable.

5.10.5 SIX SIGMA BENEFITS TO e-GOVERNANCE

e-Governance being a service oriented implementation, adopting six sigma in it will give the benefits like Customer satisfaction, Reduction of misdirected costs, Faster delivery of e-Governance service, Reliable service, Efficient and reliable internal operations, Scientific approach, Improved productivity, Employee satisfaction etc.

5.10.6 CAPABILITY MATURITY MODEL INTEGRATION (CMMI)

CMMI is widely used by software organizations throughout the world and it consists of process areas. A process area is a
A cluster of related practices in an area that when implemented collectively, satisfies a set of goals considered important for making significant improvement in that area. CMMI consists of 22 process areas which are placed under four categories. They are as follows.

<table>
<thead>
<tr>
<th>Category</th>
<th>Process Areas</th>
</tr>
</thead>
<tbody>
<tr>
<td>Process Management</td>
<td>Organizational process focus</td>
</tr>
<tr>
<td></td>
<td>Organizational process definition</td>
</tr>
<tr>
<td></td>
<td>Organizational training</td>
</tr>
<tr>
<td></td>
<td>Organizational innovation and deployment</td>
</tr>
<tr>
<td>Project Management</td>
<td>Project planning</td>
</tr>
<tr>
<td></td>
<td>Project monitoring and control</td>
</tr>
<tr>
<td></td>
<td>Supplier agreement management</td>
</tr>
<tr>
<td></td>
<td>Integrated project management</td>
</tr>
<tr>
<td></td>
<td>Risk management</td>
</tr>
<tr>
<td></td>
<td>Quality project management</td>
</tr>
<tr>
<td>Engineering</td>
<td>Requirements Management</td>
</tr>
<tr>
<td></td>
<td>Requirements Development</td>
</tr>
<tr>
<td></td>
<td>Technical solution</td>
</tr>
<tr>
<td></td>
<td>Product integration</td>
</tr>
<tr>
<td></td>
<td>Verification</td>
</tr>
<tr>
<td></td>
<td>Validation</td>
</tr>
<tr>
<td>Support</td>
<td>Configuration Management</td>
</tr>
<tr>
<td></td>
<td>Process and Product quality assurance</td>
</tr>
<tr>
<td></td>
<td>Measurement and Analysis</td>
</tr>
<tr>
<td></td>
<td>Decision Analysis and Resolution</td>
</tr>
<tr>
<td></td>
<td>Organizational Analysis and Resolution</td>
</tr>
</tbody>
</table>

208
The activities that must be performed in each process area are called practices. The two kinds of practices are Specific practices which involve the identification activities to attain specific goals of the process area and Generic practices which describe the activities which are considered important to achieve the associated generic goals. The practices proposed by CMMI are best suited for e-Governance applications to enhance the quality and best satisfies the citizen's requirements.

5.10.7 SIX SIGMA AND CMMI FOR e-GOVERNANCE APPLICATIONS

As e-Governance is taking over the various activities of society, its quality, standards and timely delivery of services became major factors. Hence today the joint implementation of the CMMI and Six-Sigma is considered with awareness. When both are to be implemented together then several planned approaches may be used and in the due course of implementation benefits of both are relished. Implementation of both is done with following observations.

- Implement CMMI process areas of e-Governance as Six-Sigma projects
- Apply Six-Sigma as the considered concept for CMMI where ever it is implemented in e-Governance projects
- Apply Six-Sigma, to achieve highly capable engineering processes
- Apply Six-Sigma to improve or optimize e-Governance improvement strategy and processes.
- Compare the e-Governance results obtained by Six Sigma using CMMI's practices.
Integrate the CMMI, Six Sigma, and all other improvement initiatives of choice to provide a standard for the execution of e-Governance project throughout its lifecycle.

In every stage of CMMI, the Six Sigma concepts can be used. The implementation of these two should be managed in an integrated fashion, so that the results of e-Governance can be enjoyed by the society.