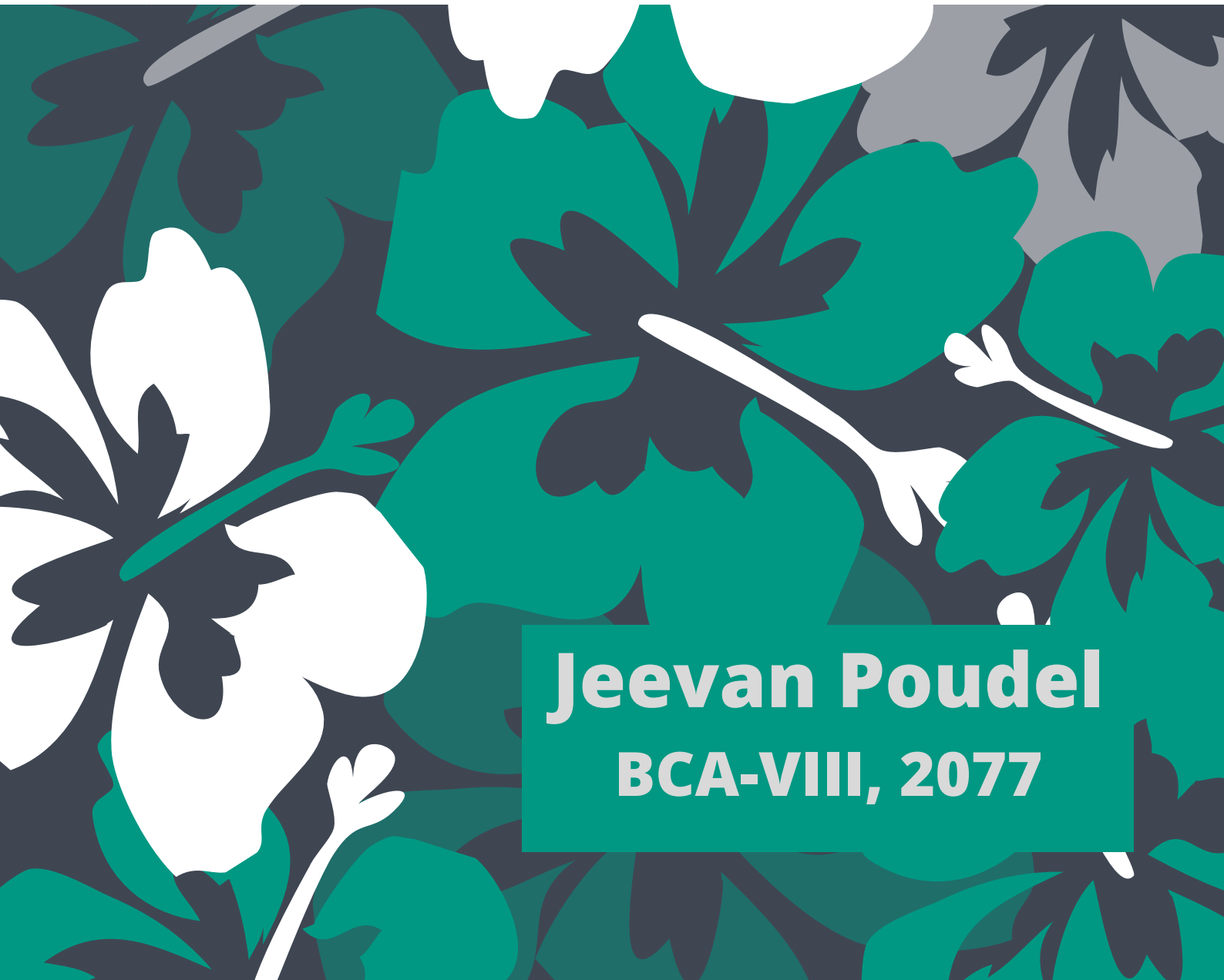
PURBANCHAL UNIVERSITY

e-Governance

(Compiled Notes)

YEAR-IV *(BCA451CO)* *SEMESTER-II*



Jeevan Poudel

BCA-VIII, 2077

Purbanchal University, Nepal

e-Governance
(BCA451CO)

(Compiled Notes)

BCA-VIII

Jeevan Poudel

श्री गोमेन्द्र बहुमुखी महाविद्यालय
वितामोड, झापा

फागुन १७, २०७७
(2021)

यो पाठ्य सामग्री तयार पार्न साथ, सहयोग र हौसला प्रदान
गर्नुहुने आदरणीय गुरु श्री जयराम चौलागाईं र मेरा सबै
साथीहरुप्रति हार्दिक आभार प्रकट गर्दछु।

CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER

1

INTRODUCTION

1.1 e-Government and e-Governance

e-government is the process of transformation of the relationships of government with its constituents - the citizens, the businesses - and between its own organs, through the use of the tools of ICT, the aim is to bring about enhanced access, transparency, accountability and efficiency in the delivery of government information and services.

Government exist for the people and for the businesses that people are engaged in. The mandate of any democratic government is to provide a set of services in an efficient, convenient, equitable and cost-effective manner so as to ensure the welfare and well being of its citizens and to facilitate the growth of economic activities. An epithet that has gained popularity in this context is *SMART government*, that is:

- **S**imple
- **A**ccountable
- **T**ransparent
- **M**oral
- **R**esponsive and

Essentially, *SMART* captures all the important attributes of good governance.

e-Governance का ५ सिद्धान्तहरु / five principles of e-governance भनेर यही 'SMART' लाई पनि भनिन्छ।

Simple

Simple would mean simplicity of the laws, rules, regulations, processed and procedures of government.

Moral

Moral government mean emergence of an entirely new system of ethical values in the polictical and administrative machinery.

Accountability

Accountability raises the question: *who is accountable to whom and in what way?*

Responsiveness

Responsiveness in the context of good governance, means to be alive to the needs of the public and to exhibit the required degree of urgency in responding to such needs. It includes quality of service and its timeliness.

An important concept developed in this context is the **Citizen Charter**. Citizen Charters are a set of assurances given by government agencies on the quality of services and the time limit for their delivery.

Transparency

Transparency basically arises out of the citizen's right to information - the right to know what decisions public institutions take and for what valid reasons. The publication of such information should be up-to-date and logically ordered for easy access.

Examles:

- assessment of taxes payable by citizens and businesses
- appointments to public posts
- disciplinary matters of employees

- selection of beneficiaries for social welfare schemes
- grant of concessions to private sector in public-private partnership scenario, and
- allocation of scarce resources among competing demands

1.1.1 e-Government

E-government has been employed to mean everything from *online government services* to *exchange of information and services electronically with citizens, businesses, and other arms of government*. Traditionally, e-government has been considered as the use of ICTs for improving the efficiency of government agencies and providing government services online. Later, the framework of e-government has broadened to include use of ICT by government for conducting a wide range of interactions with citizens and businesses as well as open government data and use of ICTs to enable innovation in governance.

E-government can thus be defined as *the use of ICTs to more effectively and efficiently deliver government services to citizens and businesses*. It is the application of ICT in government operations, achieving public ends by digital means. The underlying principle of e-government, supported by an effective e-governance institutional framework, is to improve the internal workings of the public sector by reducing financial costs and transaction times so as to better integrate work flows and processes and enable effective resource utilization across the various public sector agencies aiming for sustainable solutions. Through innovation and e-government, governments around the world can be more efficient, provide better services, respond to the demands of citizens for transparency and accountability, be more inclusive and thus restore the trust of citizens in their governments.

1.1.2 e-Governance

E-Governance is a form of e-business in governance comprising of processes and structures involved in deliverance of electronic services to the public, viz. citizens. It also involves collaborating with business partners of the government by conducting electronic transactions with them. Besides, it entails enabling the general public to interact with the government, through electronic means, for getting the desired services. In other words, e-governance means application of electronic means in the interaction between.

- government (G) and citizens (C), both ways (i. e. G2C, and C2G),

- government or business (B), both ways (i. e. G2B and B2G), and
- internal government operation (G2G)

The aim, ultimately, is to simplify and improve governance and enable people's participation in governance through mail, and Internet.

E-governance is much more than just preparing some websites. It ranges from the use of Internet for dissemination of plain web based information at its simplest level to services and online transactions on the one hand and utilizing IT in the democratic process itself, i. e. election on the other.

e-governance implies e-democracy, wherein all forms of interaction between the electorate (i. e. general public) and the elected (i. e. the government) are performed electronically. e-government, as distinguished from e-governance, comprises a pragmatic application and usage of the most innovative technologies in computer and communication technologies, including Internet technology, for delivering efficient and cost effective services, and Information and knowledge to the citizens being governed, thereby realizing the vast potential of the government to serve the citizens.

Various manifestations of e-governance initiative will be in terms of the government delivering services to citizens of transacting business, offering general information, or conducting interactions with the general public and business using such IT tools as:

- E-mail
- Internet websites publishing (including online interactive transaction)
- WAP application and publishing
- SMS connectivity
- Intranet development and usage
- Promotion of citizen access.

The advent of these other components and of Information and Communication Technology (ICT) as a highly leveraged enabling tool for delivery of services in the public and private sector has now been universally recognized. This has resulted in a redefinition of the fundamental concept of governance and also in recognizing its potential to change both institutions and delivery mechanisms of services for betterment of people.

1.2 e-Government as Information System

eGovernment is the use of IT by public sector organizations. eGovernment is therefore not just about the Internet. And e-government has been with us for many decades: long before the terminology of 'e-government' was invented. eGovernment means office automation and internal management information systems and expert systems, as well as client-facing websites.

For e-government to be a working information system, it must be seen as much more than just the technical elements of IT. Instead, it must be seen to consist of technology plus information plus people who give the system purpose and meaning plus work processes that are undertaken. We can therefore produce an initial model of an e-government system, as illustrated in Figure 1.1.

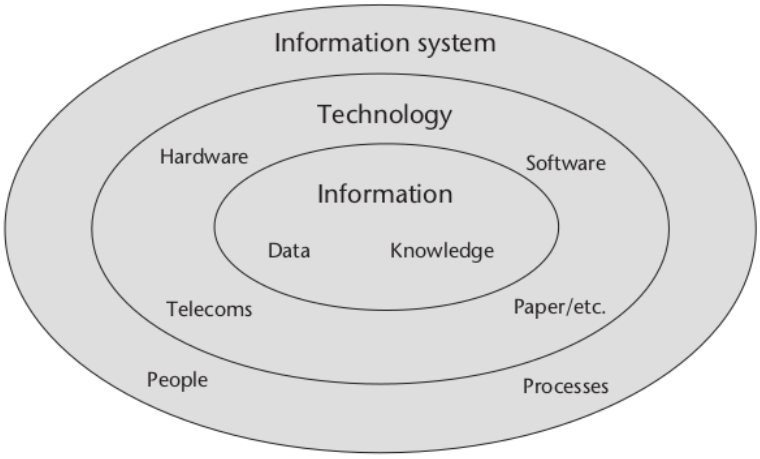


Figure 1.1: e-Government systems as information systems

IT handles data to produce information. E-Government systems are information systems. At their heart lie data and information[1]. These are handled by digital and sometime non-digital information technologies.

But this does not make a 'system'. A system is a collection of elements that works and has purpose. To understand e-government as information system, we must add in some notion of activity and purpose. That can only come if we bring people into the equation. For e-government to be working information system, it must be seen as much more than must the technical elements of IT. Instead, it must be seen to consist of technology

[1]defined as data that has been processed to make it useful to a recipient

plus information plus people who give the system purpose and meaning plus work processes that are undertaken.

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

The model in Figure 1.1 is incomplete. eGovernment systems don't just float around like satellites in space. Most are embedded within public sector organizations that provide, for example, the management systems and the organiza- tional resources that support e-government. These organizations also provide things like the political and cultural milieu within which e-government operates. Many e-government systems also reach out to other groups (citizens, businesses); a few involve other public agencies. In turn, all these groups and organizations are themselves embedded in institutional environments: a broader context of laws and values, economic systems and technological innovations that affects both the agencies/groups and the systems – including e-government systems – that serve them.

Full model of e-government must embrace these factors, as shown in Figure 1.2.

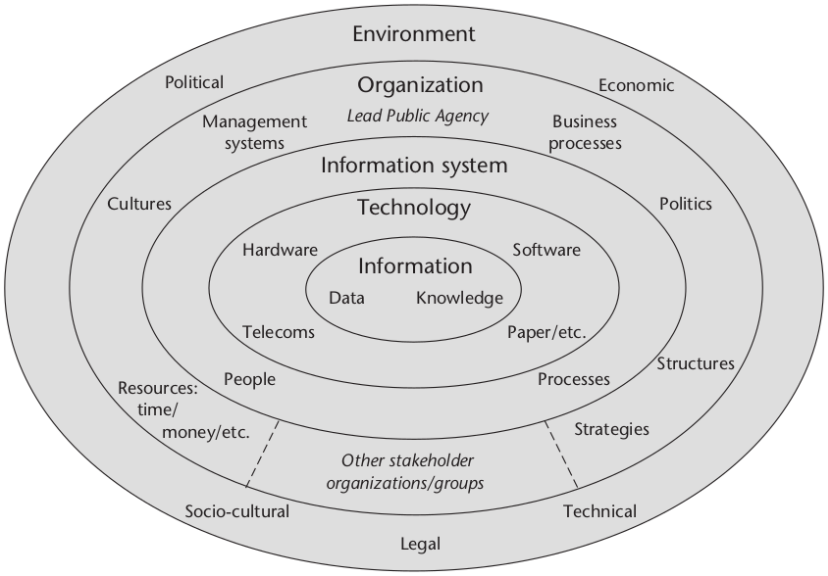


Figure 1.2: Full model of e-government systems

Figure 1.2 मा चित्रण गरिएको चित्रलाई 'onion-ring' model पनि भनिन्छ।

The ITPOSMO Checklist

In fully describing and understanding an e-government system, we could refer to every one of the 20 separate factors identified in Figure 1.2. But that would be complex. Here, we will make more use of a slightly simpler checklist of key items drawn out from this 'onion-ring' model:

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

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

In some cases, it may be important to also describe the wider context, by expanding the checklist to ITPOSMOO, adding an eighth dimension:

- **O**utside world: The political, economic, socio-cultural, technological and legal factors that impinge on the relevant e-government stakeholders.

The CIPSODA Checklist

Given that e-government systems are information systems, we can draw on one further model/checklist to help us understand e-government. This understands an e-government application in terms of its information-related tasks: a process view to go alongside the structural view offered above. These tasks are summarized by the CIPSODA checklist, illustrated in Figure 1.3.

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

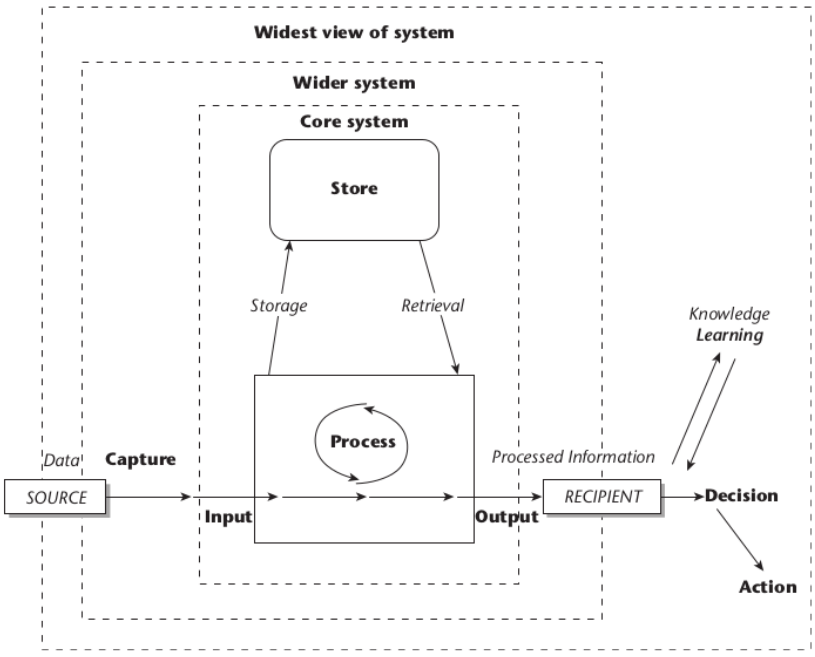


Figure 1.3: eGovernment systems as information systems: Process view

- **C**apture: Gathering the raw data necessary for the e-government system. The taxpayer obtains the basic data on their various sources of income.

- **I**nput: Entering the data onto the system. The taxpayer types the data into an e-form on the revenue agency's website.

- **P**rocess: Altering the data via calculation, classification, selection, and so on. The e-tax system uses the different tax rates for different income types to calculate the total tax owed.
- **S**tore: Holding raw and processed data on the system. The e-tax system stores all details entered and calculated about this taxpayer.
- **O**utput: Issuing the processed data. The total tax calculated is displayed to the taxpayer.
- **D**ecision: If the processed data is useful enough to be seen as information, it is used for decision-making. The taxpayer determines whether to challenge or accept the calculated tax sum.
- **A**ction: Implementation of the decision. If all is well, the taxpayer authorizes payment of the tax owed.

Note there is also an eighth task implicit within the model: the communication of data between each of the other tasks.

While Figure 1.2 uses an information systems perspective to explain what an e-government system *is*, Figure 1.3 explains more what an e-government system *does*.

1.3 Benefits of e-Government

1.3.1 Benefits to Government

1.3.1.1 Law and Policy Making

ICTs, especially the internet, enable gathering of model legislations and policies at international and national levels on any subject, and the experience of nations and regions in the implementation of those laws and policies. It is therefore possible to formulate new policies or modify/review existing laws and policies in a quicker time-frame and in a more informed manner.

e-Government, implemented extensively over a period, generated enough data and MIS that enable policy makers in better decision-making.

The strength of laws and policies depends on how widely they are disseminated. Internet is the best-suited medium for this purpose. In fact, publication of all the Acts, Rules and Regulations on websites and portals is one of the common initiatives undertaken by a majority of the nations leading in the e-Government field.

1.3.1.2 Regulation

The following areas of regulation can immensely benefit from e-Government initiatives:

- Statutory registrations of companies and business under various laws
- Taxation
- Environmental regulations
- Police
- Transportation
- Healthcare
- Education
- Food and agriculture
- Industry and commerce

Benefits in the regulatory areas could be in one or more of the following forms:

1. Better compliance due to stringent tracking and monitoring systems
2. Better revenues
3. Better coordination between related regulatory agencies (e.g. police and transportation) due to shared databases
4. More transparency in enforcement of laws

1.3.1.3 Provision of Services-Electric Service Delivery (ESD)

Electronic Service Delivery (ESD) is beneficial to the citizens as well as government. Following are the benefits of ESD to the government.

- *Better image*: Speed, efficiency, transparency and convenience arising out of ESD enhance the image of government.
- *Cost cutting*: The automation process reduces manpower costs, besides costs of accounting, compilation, reporting and review.

1.3.2 Benefits to Citizens

The cost citizens has to incur on ascertaining the forms and procedure appropriate to the service needed, travelling to the designated government agency or to an intermediary/agent multiple time are where citizen lose their valuable time and money. By using e-government setup these costs can be reduced or eliminated. Besides cost reduction, the other benefits to the citizen can be in the form of:

(a) increased transparency leading to reduced corruptions.

(b) better planning of personal and professional work arising out of definiteness in dealing with the government.

(c) better quality of life as a result of the use of ICT in areas such as health, education, employment, welfare and finance.

(d) easy access to information on government agencies and programmes.

(e) multiple delivery channels to choose from, thus adding to convenience and

(f) facilities like single-window and Single-Sign-On that remove the complexities of visiting multiple government agencies or websites.

1.3.3 Benefits to Business

1.3.3.1 Increased Velocity of Business

With the digitization of the G2B interface, the velocity of business increases. Ease of filing returns and enhanced speed in securing the various permits and licenses through electronic single windows are examples.

1.3.3.2 Ease of Doing Business With Government

e-procurement provides a convenient Internet-based medium for online registration of suppliers, bidding for works and projects, and tracking the status of their award.

1.4 e-Government Stages of Development

The theoretical progression of e-Government in any country or state is along *four stages* which indicate the extent of benefits that the stakeholders get through the e-Government projects prevalent in that country or state. These are represented schematically in Figure 1.4.

1.4.1 Information

This is the initial stage of web presence. A few websites are launched that contain limited and static information, which is updated more frequently with increasing usage and customer pressure. The information may be limited to basic functions, facts and figures and contact details of government

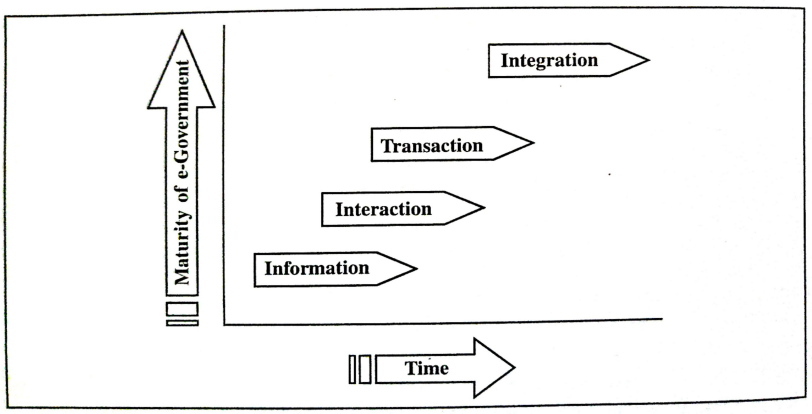


Figure 1.4: e-Government systems as information systems

departments and agencies. The information stage does not call for any efforts at 'Computerization' of the backend.

1.4.2 Interaction

In this stage, the citizen can *interact* with the government agencies in a 'one way street' manner. The citizens can download forms, file forms, returns and complain online, with government agencies. This stage calls for building capacity and systems in the backend government agencies to receive the request send by the citizen online and to process in sequential and accountable manner. The interactive website reduce the tedium of the citizen partially by enabling them to save at least one step in dealing with government agencies.

1.4.3 Transaction

This is a much more difficult stage to reach. In the transactional stage, the citizens can go through a full cycle of fulfillment of their request. It is a two-way street. Complete and secure transactions such as online payments for utility bills, taxes, fees, registration, renewals, obtaining permits, licenses and certificates are typical examples of transactions. e-Procurement, Online customs clearance, single window and single-sign-on are more sophisticated examples of this stage. This requires extensive system study, establishing data centers, disaster recovery and management system. The services have to be delivered on a 24×7 basis, the services should be citizen centric and should reflect the transformation that is the hallmark of e-government.

1.4.4 Integration

This is yet the Utopian[2] stage of e-government. This stage envisages[3] offering government information and services in an integrated manner not only from government view but also from citizen and business side. The key events in the citizen's life are- birth, admission to school, admission to college/university, employment, housing, marriage, shifting of job/house, medicare, senior citizenship and death. The key events of business are registration of a firm/company, securing all clearances for setting up business/industries, filing of returns, payment of taxes and winding up.

1.5 Online Service Delivery and Electronic Service Delivery

1.5.1 Online Service Delivery

Online service delivery is the system of e-government by providing information and other various services through the means of Internet. Most services can be provided by online and services are available anywhere anytime but only the limitation is lack of availability of Internet to all places and not every citizen are computer-literate. Also, government have to initially invest large budget for establishing, utilizing and securing ICT system for online service delivery.

1.5.2 Electronic Service Delivery

Electronic service delivery means providing the services to citizen and business electronically without Internet i. e. Television, Radio, Telephone, SMS system etc.

[2]An idealistic (bust usually impractical)
[3]Form a mental image of something that is not present

CHAPTER

2

PUBLIC-PRIVATE PARTNERSHIP FOR E-GOVERNMENT

Public Private Partnership (PPP) is a different method of procuring public services and infrastructure by combining the best of the public and private sectors with an emphasis on value for money and delivering quality public services.

The concept of PPP has been brought into operation in the construction and operation of public infrastructure projects like bridges, airports, highways, hospitals, etc.

PPP is a reform that is a 'generation next' to privatization. Privatization is the process of involving the private sector in the ownership and management of of ongoing and existing projects and business of the public sector. In PPP, the private sector partner is induced into a project right from the stage of initiation to completion and management.

Why PPP for e-Government?

Combining Accountability With Efficiency

- PPP for e-government would combine the accountability and domain expertise of the public sector with the efficiency, cost-effectiveness and customer-centric approach of the private sector.

Complexity and Size of e-government

Since many agencies are managed by government, its strucute is huge and complex but government does not have sufficient resource to manage such complexities, private sector could raise *unlimited* resources.

Pace of Implementation

Government cannot plan for implementing projects one after the another because it would be almost impossible to maintain all the projects smoothly.

In order to maintain a high pace in implementing e-government, government should join hands with the private sector.

2.1 G2B Project

- e-procurement
- G2B portal

2.2 G2C Project

- Citizen service portals
- Integrated service centers
- Agency service centers
- Networks of kiosks

2.3 PPP Forms

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

2.3.1 Joint Venture (JV) Model

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

A JV model is preferred option for projects involving

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

(b) setting up of infrastructure with steady returns envisaged in long term e. g. a State Data Center.

(c) handling of sensitive data and information relating to citizen, businesses and government and

(d) close coordination with and cooperation from a host of government agencies.

In Joint Venture the government share varies from 51% to 11% which can be in cash but also can be in the form of tangible assets like land, building, equipment or in the form of intangible assets like right to access government information and databases for providing e-services.

In Nepal, some hydro projects are under construction on JV model between government and public.

2.3.2 Build-Own-Operate (BOO) Model

- In this model, the selected partner designs, develops and implements the projects, most often, entirely at its cost and operates the system for a pre-specified period called *concession* period.
- The revenue model of the project is either based on transaction charges (paid by the citizen or the government) or EQI/EMI(Equated Quarterly Installment/Equated Monthly Installment) paid by the government to the operator/service provider.

- The BOO model is suitable for projects that involve setting up of physical infrastructures such as service center(s) for delivering services to the citizens.

Example are projects related to:

- driving licenses
- vehicle registration
- provision for integrated services

The important aspects in drafting Request For Proposal (RFP) for BOO Project are:

(a) to determine period of the arrangement during which partner is authorized to deliver the services, and

(b) The bid parameter dealing with transaction charges and/or EQI/EMI to be quoted by the competitive bidders.

The BOO model is usually adopted in e-Government projects that deploy time-tested technologies and have a fairly reliable revenue mode.

2.3.3 Build-Own-Operate-and-Transfer (BOOT) Model

This is almost identical to BOO except that the government exercises ownership of the assets created by the partner at the end of the project.

This model is adopted where the technology is time tested and the ICT assets are expected to outlast the concession period.

2.3.4 Application Service Provider (ASP) Model

In this model the government contracts to avail[1] the services of the partner for delivery of services as per mutually agreed service levels and commercial terms. The revenue model is typically transaction based. The ASP model is suitable to e-government initiatives that involve:

(a) a requirement to launch the services in a short time frame.

(b) the technology is not complex and is widely accepted and practiced in the private sector, and

[1] Take or use

(c) the nature of information is not so sensitive or critical to governance.

Examples of ASP model are:

(i) design and hosting of websites that provide fairly static information to the citizens.

(ii) provision of simple services like downloading/filing of forms, and

(iii) provision of MIS services in the G2G arena to the government agencies.

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 the ICT infrastructure already setup in the private sector and thereby reducing the transaction cost to the government/citizen. The ASP model also saves the government agencies of the hassles of designing complex technology and partnership models.

2.4 Issues in PPP for e-Government

Though there are many advantages of PPP, if proper negotiation is done. But both have their own interest to earn more benefits which may threaten PPP relationship. Some issues are:

2.4.1 Lack of Congruence in Objectives

The degree to which the public and private sector partners align themselves along sharing the investment and control. Both must commit to developing an understanding of each others objectives but failing in such understanding and only focus on own interest creates lack of congruence in objectives and may fail the relationship.

2.4.2 Risk and Control

In every business there is risk and control mechanism. Most often, governments attempt to transfer risk to the partner without passing on the related control quoting 'public interest' as the reason.

2.4.3 Clash of Cultures

The organizational culture of private and public sector differ widely in all parts of the world which is bound to result in conflicting situation. The private partners tend to look at the government employees as bureaucrats with antiquated ideas that have outlived their time.

2.4.4 Monopoly

In some cases, only one partner is suitable in areas such as e-procurement, country or state portal, data center, gateway and the like. This is likely to result in a situation of monopoly- the monopoly of the state being replaced with the monopoly of the private partner and more importantly, *monopoly of a particular technology.*

The following methodology is recommended to mitigate its impact.

Operational Monopoly

The *operational monopoly* can be handled by defining the commercial features of the contract unambiguously while notifying the project to an open bid. The following factors are to be considered:

1. Projected customer base and transaction volume
2. Length of the concession period
3. Fee structure of the existing services
4. Price elasticity of the new services
5. Capacity for growth.

Technology Monopoly

The *technology monopoly* can be mitigated by prescribing open standards in conformity with the technology architecture approved by the government and ensuring that there is scope for developing interfaces with other systems that may be developed concurrently or in the future.

2.5 Citizen-Centric Approach to e-Government

Citizen-centric eGovernment services are designed to deliver increasingly cost-effective, personalized and relevant services to citizens, but also serve to enhance the democratic relationship, and build better democratic dialogue, between citizens and their government, which then enhances the practice of citizenship within society.

1. It is necessary to look at e-government from the citizen or customer's point of view and design the front-end and the back-ends to the extent required to fulfill the requirement of citizen/customer, i. e. e-government initiatives should not be system driven or supply-driven but should be demand-driven.

2. The e-Government projects can be classified as *core* and *non-core*. Core projects are those, that can be used by all departments across the state and with significant impact on key stakeholders like citizen, businesses and employees.

3. The e-Government projects can also be categorized as *commercial* and *non-commercial*. Commercial projects are those that permit a viable public-private partnership model to be implemented with the least outgo from the public exchequer[2] for implementation.

[2]The funds of a government

CHAPTER

3

ICT INFRASTRUCTURE FOR E-GOVERNMENT

3.1 Network infrastructure

Network infrastructure means the infrastructure that helps to connect computing devices within the office, other offices or connected to the world using internet. Network infrastructure includes networking devices like switch, router, networking cables, internet, intranet etc.

3.2 Computing Infrastructure

Computing infrastructure means availability of computers, laptops and other related devices which are needed for day to day computerized work in the office and providing various services.

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

- Again, like communication infrastructure, there is a high order of disparity in availability, affordability of computing devices in urban and rural areas, particularly in developing countries.
- Further, in rural areas, due to lack of basic infrastructure such as electricity, telephony, it may not be worthwhile for the people to have computers, even if they could afford it.
- To extend the reach of government services and address the wide range of citizens, governments all over the world are setting up common / shared / community infrastructure in the form of community information center, Internet kiosks etc.
- Government should also consider, making their services accessible from various other media/devices such as basic telephones, mobiles, cable TV network, PDAs and many other hands held devices.

3.3 Data Centers

Data centers is a place where many dedicated computers, servers and storage are available for mass storage of data. All public or private offices can backup their important data in secure way in least cost and prevent any loss of their data from disaster or failure of their system. In Nepal there are two data centers GIDC and DOIT.

- In the era of e-governance, government is expected to deliver its services to the citizens on 24×7 bases. To achieve this, the government has to set up a sound and stable infrastructure operational round the clock.
- Internet Data Center is a facility which provides extremely reliable and secure infrastructure for running Internet operations on a 24×7 basis. It shall not at all be cost effective if each department starts setting up its own data center as running a high class Internet Data Center needs a lot of recurring resources.
- It is, therefore, suggested that the government may set up a high grade Data Center at a National level to be used by all entities of the government.
- All departments should, in turn, establish high speed connectivity with the data center so that they can manage their applications from their own premises in a secured manner.

- In cases where the country is large and the government feels that one Internet Data Center may not suffice, it could decide to set up multiple Data Centers.
- However, the number of data centers should be optimized to the extent possible primarily due to the high recurring operative costs as well as scarcity of skilled resources.
- As the pace of e-government picks up nationwide, besides delivery of services, Government may also have to set up data centers to share the large scale/special purpose resources for development of the systems.

3.4 e-Government Architecture

There is no commonly agreed definition of e-Government architecture. The result is how the different countries states it. E-government Architecture generally consists of three components:

1. Service Architecture
2. Process Architecture and
3. Data Architecture

3.4.1 Service Architecture

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

3.4.2 Process Architecture

(i) Lists the various processes to be followed for rendering different services, independent of their association with one or more services.

(ii) These processes are then further grouped in various categories and detailed rules/procedures are defined for executing each of the processes.

(iii) This brings a lot of standardization across services and promotes interoperability as well as reuse of process components.

(iv) Processes could be Content Management, Citizen Registration, Personalization, Online Form Submission, Electronic Payment etc.

3.4.3 Data Architecture

(i) Deals with the data associated with various Government Services, as described in service architecture.

(ii) In Data Architecture, we enlist all the data elements needed/associated with above service and then define meta-data about each data element.

(iii) This meta-data information includes the standard Nomenclature for each data elements, their type, size, format, default value, valid value range, owner etc.

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

3.5 Interoperability Framework

- The Interoperability Framework aims to define the set of specifications to facilitate Government systems to communicate and interoperate with other systems, both within Government and external to it, efficiently and effectively.
- By bringing together the relevant specifications under an overall framework, ICT management and software developers have a single point of reference whenever a need arises to locate the required interoperability specifications that should be followed for a specific project.
- By adopting these interoperability specifications, system designers can ensure interoperability between systems while at the same time have the flexibility to select different hardware, systems and application software to implement solutions.
- In order to attain this objective, the Government needs to be perceived as a single entity, with seamless flow of information across individual ministries and departments as necessary.
- Framing of policies and specifications for Interoperability Framework should be followed up with provision of support, guidance on best practices, toolkits and agreed schema.

- The entire strategy to implement good e-government should be viewed in long-term perspective and hence must be supported by vigorous processes.
- The development of Interoperability Framework must therefore be reviewed and updated on a continuous basis.

e-Government Interoperability Framework (e-GIF)

e-GIF is a set of guidelines and technical specifications, designed to promote interoperability between various e-government systems, though developed independently by various agencies. In the words of Mr. Douglas Alexander, in his foreword to the e-GIF Framework (Version 5.0),

> "in terms of e-service delivery, compliance with the (e-GIF) Framework is essential for the public good... the Framework aligns government with the rest of the industry and serves as a basis for reducing the costs and risks associated with carrying out major IT projects"

The key policy decisions that have shaped the e-GIF are as follows:

- Align with the **Internet technologies** and specifications, for all public sector information systems.
- Adopt **XML** as the primary standard for data integration and presentation tools,
- Adopt the **browser** as the key interface.
- Adopt **metadata** to government information resources.
- **Mandate** e-GIF throughout the public sector.

The e-GIF specifications are driven by integrability, market-support, scalability and openness of the technologies prescribed. The scope of e-GIF specifications has been limited to four key ares of technology, viz.

- Interconnectivity,
- data interpretation,
- e-services access and
- content management

CHAPTER

4

E-GOVERNMENT READINESS

e-government takes root and grows when a country, state or agency is *e-ready*.

e-Readiness

According to Harvard Business School,

> an e-Ready society is one that has the necessary physical infrastructure (high bandwidth, reliability and affordable prices). It should also have an integrated, current ICT's throughout business communities (e-commerce, local ICT sector), and government (e-government). Other important aspects are strong telecommunications competition, independent regulation with a commitment to universal access, and no limits on trade or foreign investment.

In short, e-readiness measures a nation's capacity to participate in the digital economy. While e-readiness is a larger concept that measures how a nation comprising citizens, businesses and government takes advantage of the digital revolution, 'e-government readiness' relates to how the process involving the government are transformed using the tools of ICT. In other words, e-readiness touches upon the state of all interface - G2G, G2B, B2B,

B2C and C2C, while e-government readiness is concerned with only the first three interfaces.

4.1 e-Readiness framework

Following list shows component, sub-component and indicators of e-readiness.

1. **Policy**
   (a) ICT Policy
      - Communications Policies
      - Policy on ISP
      - Incentives to ICT Industry
      - Recognition of Quality
      - Facilitation of Growth & Promotion of Exports

   (b) E-Government Policy
      - E-Government Vision
      - Prioritization of Services
      - PPP Policy
      - Policy on ESD (Electronic Service Delivery)

   (c) Architecture & Standards
      - Functional Architecture
      - Technical Architecture
      - Technical Standards

   (d) Security Framework
      - Security Policy
      - Privacy

   (e) Regular Framework
      - Cyberlaw
      - IPR Protection

2. **Infrastructure**
   (a) Networks
      - National Backbone(s)
      - Distribution Networks

- LANs & WANs
- Satellite & Wireless Networks

(b) Access

- PC Penetration
- Internet Penetration
- Last Mile Connectivity

(c) ICT Hardware

- Data Center
- e-Government Gateway
- Payment Gateway
- Public Key Infrastructure

3. **Resources**

(a) Political Resources

- Leadership & Vision
- Continuity of Support to ICT Sector

(b) Human Resources

- IT Education & Training Institutions
- Expenditure on R&D in ICT

(c) Employee Resources

- Champions of ICT
- Chief Information Offices
- Access to PC & Internet at Office

4. **Usages**

(a) Usage by Citizen

- e-Mail & Internet Usages
- e-Literacy

(b) Usage by Businesses

- e-Commerce
- e-CRM; e-SCM
- e-Procurement in B2B & G2B Areas

(c) Employee Resources

- No. of Websites/Portals
- No. of e-Services; e-Transactions
- No. of e-Government Projects
- Extent of G2G Usage

The e-readiness framework consists of assessing readiness along four fronts:

- policy,
- infrastructure,
- resources and
- usages.

Each of the four components consists of 3-5 sub-components that enable a deeper understanding of the state of each of the major components. A set of 43 indicators is suggested as a drilled down of the sub-components to enable quantitative and qualitative assessment of e-readiness.

It is possible to develop a methodology to asses the e-readiness of a country or a state, through a structured questionnaire, administered to a representative sample population of the citizens, companies and government agencies and supplementing the same with the macroeconomic data available with regulatory bodies, research institutions and industry associations. The following questionnaire is suggested as a starting point. It can be improved upon and customized to suit varying circumstances.

4.1.1 Policy

ICT Policy

- Does the country (State) have an ICT policy? How old is it? How contemporary is it?
- Does the country (State) have a telecommunications policy? Does it promote competition?
- Does the country have a policy on ISPs (Internet Service Providers)?
- Does the State provide sizeable incentives to the ICT sector in the form of tax concessions, allocation of state lands at a concession?
- Does the state promote exports of ICT products and services?
- Are there awards instituted for excellence in ICT sector?

e-Government Policy

- Is there a document that specifies the state's e-government vision and strategy?
- Is there clarity on the priorities in implementation of e-government? Is there a 5- or 10-year perspective plan, broken down into annual action plans with clear quantitative and qualitative targets?
- Has the state laid down a transparent policy on Public-Private Partnership for e-government? How many PPP initiatives are ongoing/completed?
- Is there a policy on ESD that creates an open framework for development of multiple channels?

Architecture and Standards

- Has the government published a document that sets out the functional architecture or business process architecture?
- Is there a document that prescribes standards in all the technology areas like application development, databases, middlewares, networks, storage, etc. ?
- Has the government published a technology architecture that is based on open standards and permits development of IT systems in an interoperable manner and a seamless integration with national and global systems?

Regulation

- Is there an overarching cyberlaw at the national level that confers legal status to electronic transactions and documents?
- Is there a law on regulation of digital signatures and encryption?
- Is there a law to protect Intellectual Property?
- Is there a law on privacy that protects the information of citizens and businesses captured by the government and private agencies, against unauthorized use?
- Is there a statutory regulator for the telecom sector that promotes competition?

- Is there an effective legal machinery to tackle the problem of piracy of ICT products?

4.1.2 ICT Infrastructure

Networks

- Are there at least two major national networks that connect all the major cities?
- Are there two or three distribution networks to connect all towns and all villages?
- Do the federal and state governments and their agencies have WANs of their own?
- Do the public offices and enterprises have LANs that use State-of-the-art switches and routers?
- Is there effective usage of satellite and wireless networks in government and business?

Access

- What is the PC penetration in terms of a PC per 1000 population? What percent of households have PCs?
- What is the Internet penetration in terms of Internet accounts per 100 of population?
- What is the technology adopted to connect the last mile? Dial up? Optical Fiber Cable? Wireless?

ICT hardware

- How many data centres are established in the country?
- Does the country have an e-government gateway?
- Is there an e-payment getaway?
- Does the country have a PKI?

4.1.3 Resources

Political Resources

- Is there a document at national level that describes the ICT vision of the country?
- Is there a political consensus on the promotion of ICT in the country?
- Are there champions of ICT and e-government at the national and state levels among the political executives?
- In the last 10 years, how often has political support been given to the ICT sector?

Human Resources

- Is the country or state self-sufficient in IT graduates?
- How many IT training institutes operate at the national level, outside the formal education system?
- What is the percentage of turnover spent on R&D in the ICT sector?
- How many institutions of excellence that have national and international reputation exist in the IT sector?

Employee Resources

- What percentage of enterprises (other than SMEs) have qualified Chief Information Officers?
- What is the percentage of government enterprises- federal and state- having CIOs?
- What is the percentage of employees having access to a PC and Internet at office — in the public and private sectors?

ICT Resources of Private Sector

- How many ICT companies are active in the country/state?
- How many of them partner the government?

Financial Resources

- What is the total ICT budget of the Federal, State and local governments?
- What is the annual IT expenditure of the private sector?

4.1.4 Usage

Usage by Citizens

- What is the rate of e-literacy among the citizens?
- What is the extent of e-mail usage and Internet browsing among citizens?
- What percentage of citizens use e-service over the Internet in preference to over-the-counter?
- What is the share of e-buying in the total consumer spend?

Usage by Business

- What is the share of e-commerce in the overall business?
- What percent of major industries and business have adopted eCRM, eSCM and e-procurement?
- What is the level of trust in the net among business people?

Usage by Government

- What percent of G2C and G2B services are offered electronically?
- What percent of G2G, G2B transactions occur electronically?
- How many enterprise-wide e-government projects are operational?
- What percent of government agencies have websites/portals that are regularly updated and used by the citizens?
- What percent of government employees use PC and Internet for official work?

It is a long and elaborate questionnaire. The answers to most of these questions can be qualitative to begin with. Where quantitative responses are required, a sample survey would be the best. It is advisable to adopt a system of weightages to assess the overall e-readiness of a country/state or enterprise.

4.2 Steps to e-Government Readiness

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

Step 1: Articulate the e-government vision and strategy. Prepare a five-year perspective plan.

Step 2: Review the Telecommunication policy, to promote an open, competitive environment for creation of national and sub-national networks.

Step 3: Prepare a list of G2C and G2B services that citizens and businesses need to be provided electronically.

Prioritize the services.

Announce a policy on electronically services delivery.

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

Prescribe standards for security.

Step 5: Initiate statewide e-government projects adopting the pilot approach. Ensure these are part of the 'big picture' developed in *Step 4*:.

Step 6: Design and implement an appropriate CIO program.

Implement change management programs across all major government agencies.

Step 7: Ensure that all government agencies earmark[1] 2-5% of their budget to e-government.

Announce a PPP policy for e-government and take up a few projects adopting the PPP Model.

Step 8: Establish a government–wide WAN for data, voice and video for G2G applications, adopting a PPP model.

Step 9: Enact a cyber law that gives a legal validity to all electronic transactions and records and permits use of digital signatures for authenticating messages and documents.

Publish polices on security and privacy for e-government.

Step 10: Establish data centers for e- government using the PPP model.

Design and establish an e-government gateway at the State Data Center.

4.3 Issues in e-Government Readiness

Getting a country into a stage of e-readiness requires a mulltipronged[2] effort. While it is possible to adopt a structured approach, it is fraught[3] with several problems. It is necessary to look at three issues which are crosscutting in nature:

- people readiness,
- reform readiness, and
- readiness for sustainability.

4.3.1 People readiness

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

1. Readiness to *think*
2. Readiness to *learn*
3. Readiness to *act*
4. Readiness to *transform.*

[1] designate (funds or resources) for a particular purpose

[2] having several distinct aspects or elements

[3] (of a situation or course of action) filled with or likely to result in (something undesirable)

4.3.1.1 Readiness to Think

Readiness to think of e-government is to do with the change of mindset and is by far the most difficult one to achieve.

4.3.1.2 Readiness to Learn

Readiness to learn is easier to come by. It can be ushered[4] in through a set of attractive training programs coupled with visits to successful e-government projects and interaction with people running the project and those benefiting from it.

4.3.1.3 Readiness to Act

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

4.3.1.4 Readiness to Transform

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

4.3.2 Reform Readiness

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

4.3.3 Backend Readiness vs. Front-end Readiness

One of the classic conflicts that arises in the course of a serious implementation of e-government is the one between 'backend readiness' and 'front-end readiness'. By 'backend readiness' we mean the following tasks:

[4]show or guide (someone) somewhere.

Developing Backend Systems

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

Establishment of Iinfrastructure

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

Readying the people

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

Front-end

Frontend readiness means the following:

- Creation of a delivery channel policy
- Establishing service centers/kiosks
- Creation of websites and portals

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

CHAPTER

5

SECURITY FOR E-GOVERNMENT

Security is a generic word used to describe the defense mechanism to be set in place by all users of ICT to ward off the attacks on their information assets-whether in storage or in transit - and to mitigate the impact in the event of an attack. Given the ingenuity of ICT users (abusers!), the attacks can happen in several forms and so the defense mechanisms have to be sufficiently strong and comprehensive.

5.1 Challenges of e-government Security

As we know the e-Government provides services to citizen, business, employees and stores the data and information of almost all aspects of the government and the country, there is always danger of access by unauthorized people through hacking. There must be mechanism to provide security so some of the challenges of e-Government security are as followsChaulagain, 2021:

5.1.1 Need for a Good User Experience

A good user experience is one of the factor conducive to the success of e-Government initiatives. The users can be internal users i. e. the employees

of the agencies that operate and manage ICT systems at the backend, or the end users, i. e. citizens and businesses that access e-services. Both sets of these users want as few hassles as permissible while gaining access to system and services who want to do their work in few clicks. This requirement places serious limitations on the number and type of security controls that can be put into the system without loosing user interest.

5.1.2 Multiple Legacy Environments

Governments may have many legacy system each with own security subsystem. Creating a comprehensive security framework that can inter-operate between such diverse system can be a challenge. Similarly, multiple application system demand varying degrees of rigor in security implementations, depending on the varying threat perceptions. A blanket of security mechanism is not always the best.

5.1.3 Ever Expanding Domain of e-Government

With governments eager to deliver more and more services online to a larger client, the boundary that needs to be protected is ever-increasing and so also the nature and intensity of attacks with which the expanded domain is threatened. This adds a new dimension scalability of the security solutions designed in the preliminary stages.

5.1.4 Wide Range of Access Needs

The users within the government agencies are a peculiar lot. They need as much flexibility in their operations as in the paper-based system — if not more! Failure to realize this and provide for the same might act as a strong de-motivator. For instance, users would expect to access the backend system from anywhere and at anytime. They would like access to be provided at the workstation in the office and through the laptop while at home or on travel. They would like speech-recognition software to be deployed, so they can talk to the computer rather than type into it! These requirements bring in special vulnerabilities that need to be addressed by the security designers.

5.2 An Approach to Security for e-Government

A rational approach to security start with two questions -"security of what?" and "security against what?" These are, incidentally, the two questions to be answered by any agency while undertaking the first steps in e-security - the self-assessment stage.

5.2.1 Security for What?

Security is all about safeguarding the ICT assets of an organization. The assets in the portfolio could be internal assets of the organization or external assets. While the internal assets are easy enough to visualize, the external assets that lie outside the 'perimeter' of the organization include the assets of the clients, remote users and business partners who need to communicate and collaborate with the organization day in day out. The ICT assets themselves can be of a wide variety including the following:

Data

Data in the form of data on the organization, its transactions, sensitive data relating to citizens and businesses such as the socio-economic data of citizens and business returns, data relating to properties of individuals and their titles and charges thereon, medical data of citizens, data of educational institutions and social security data. The data can be in individual databases, data marts or in data warehouse.

Information

Information in the form of processed data, such as processed tax returns, driving licenses, medical claims, annual business returns, websites of agencies, directories of users, work-flow processes etc.

Knowledge resources

E. g. patents, Acts, Rules and Regulations, research papers, reports, meta-data schema, standards and specification, most of which may contain valuable intellectual properties.

Programs

Programs such as e-government applications that provide services to millions of citizens and thousands of businesses, operating systems, e-mail systems and web servers. Most of them contain thousands of person years of efforts behind them.

Hardware

Hardware such as PCs, servers, routers, switches, data centers.

Networks

E. g. LANs, WANs, and wireless networks.

5.2.2 Security against What?

The threat to security of ICT systems may come from many sources and in many forms. It is necessary to identify these threats, in the context of a particular e-government project or of the environment in general. What are the sources of threat to e-government? The sources can be internal or external to the government agency.

5.2.3 Internal Sources of Threat

Government employees

Government employees working within e-government projects may misuse their access privileges to secure financial gains or disgruntled employees may try to sabotage the program to spite the government and/or to retain their vested interests.

Employees of the private partners

Employees of the private partners of e-government operating the systems in a PPP arrangement may resort to such a misuse as above.

Customers of the e-government programs

Customers of the e-government programs may attempt to access the databases for financial gains.

5.2.4 External Sources of Threat

Professional hackers

Professional hackers who have the requisite technical skills to break into e-government systems, are perhaps the biggest threat. They may not expect any financial or other gains but the sadistic pleasure of disrupting citizen services.

Criminal organizations

Criminal organizations which are inimical[1] to the government.

Terrorist organizations

Terrorist organizations that want to destabilize economies predominantly dependent on digital systems.

Intelligence and investigation agencies

Intelligence and investigation agencies that want to secure sensitive and classified information from government agencies.

5.2.5 What are the Types of Threats?

Threats to ICT assets may be of different types and varying intensities and impact values. As a corollary[2], the attacks on security of systems can be in different forms including the following:

Defacing of web sites

Defacing of websites and filling the home pages with objectionable material.

Hacking into servers

Hacking into servers and stealing valuable data and information.

Damage

Damage to critical databases and applications.

[1] Not friendly

[2] A practical consequence that follows naturally

Denial of Service Attack(DOS)

Denial of Service Attack (DOS), which involves flooding the government portals with millions of requests at business-critical hours to deny the service to genuine users.

Virus attack

Virus attack directed against a particular government agency or broadcast without direction, which may have the effect of corrupting data or application programs and is usually associated with slowing down or even breakdown of networks.

The damage to ICT assets need not always be a result of such malicious attacks as above. It can be occasioned by accident, incorrect usage of the systems. Can be a result of power fluctuations or outages, natural calamities such as floods, earthquakes, fire or vandalism.

The UK Government, in its *e-government Security Framework*, lists 18 types of attacks and threats to e-government assets.

1. Unknown outsider attacks
2. User fraud
3. Insider attack
4. Privileged insider attack
5. False identity
6. Impersonation
7. Unauthorized disclosure
8. (Misuse of) revoked rights
9. Theft of access token
10. Duplication of access tokens
11. Capture of access credentials
12. Denial of service attack
13. Misinformation and propaganda
14. Breach of anonymity
15. Breach of accountability
16. Failure to recover business information
17. Loss or theft of monetary value
18. Challenges to system veracity[3]

5.3 Security Management Model

Security of e-government systems has to be managed systematically, comprehensively and continuously. Figure 5.1 shows a model for understanding the

[3]accuracy

various elements in such a security environment.

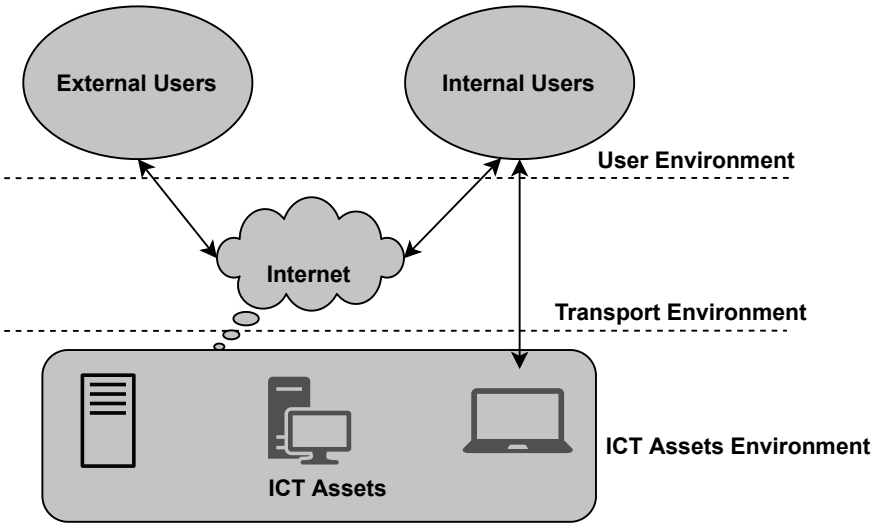


Figure 5.1: Security Environment.

The security environment consists of three distinguishable areas or environments, each of which is subject to different types of threats and consequently needs different security treatment:

- The *User Environment*
- The *Transport Environment*
- The *ICT Assets Environment*.

Table 5.1 brings out the essence of the security model

Table 5.1: Security Mode of e-Government.

Environment	**Management systems**	**Management tools**
User Environment • Internal users • External users	• Identity Management • Access Management • Interaction Management	• Passwords • Digital identity token • Access Control Lists (ACL) • PKI • Biometrics • e-government gateway
Transport Environment • Within LAN, WAN • Over the Internet	• Secure Communication System • Cryptographic Systems	• Government secure Intra-net • Virtual private networks • Government Secure Internet (GSI) • Encryption
ICT Assets Environment • Tangible assets • Intangible assets	• Physical Security • Electronic Security	• Firewalls • Intrusion detection systems • Anti-virus systems • Disaster recovery site

From the security perspective, the e-government environment can be imagined to consist of three portions:

- the *User environment*
- the *Transport environment* and
- the *ICT Assets environment*.

Users can be internal or external. Transport can be over private or public networks. ICT assets can be Tangible or Intangible.

5.3.1 User Environment

Security Management of user environment involves asking three basic questions of individuals seeking to access the information system or to interact with it.

1. *Who are you?*
2. *What are you permitted to do with the system?*
3. *What are you accountable for in your interactions with the system?*

This is the objective of the three management systems shown in Table 5.1 -Identity Management Systems, Access Management Systems and Interaction Management Systems.

Identity Management Systems

The objectives of an Identity Management System are:

- To create unique *digital identities* or credentials to all legal persons—citizens and businesses—after establishing their existence and identifying them with reference to name, date of birth, etc.
- To create and manage directories which link the digital identities with the real world identities and provide for their *accessibility* to all other persons seeking to communicate with them.
- To create and manage ICT systems which ensure that the digital identities are *secure*, i. e. they are not stolen, easily tampered with or 'broken into'.

- To *revoke* the digital identity of a person when its confidentiality has been compromised or such identity is not otherwise required, by virtue of the death of such person or cessation[4] in the role or office.

Examples of Identity Management Systems are:

Username and password management system A simple and 'conventional' *username and password* management system together with appropriate directory management services. The following guidelines are provided in this regard:

(a) Government agencies should *clear-cut password policies* that prescribe things like the minimum password length, complexity of the password in terms of mandatory combination of alpha-numeric and special characters, life period of a password that forces users to change the password, restriction on adopting the same password time and again and procedures for revocation of password.

(b) It is advisable that the directory be maintained securely and centrally so that it is available to all authorized users.

(c) Lightweight Directory Access Protocol (LDAP) compliance is preferable when a very strong security is not required.

(d) Implement a fault-tolerant solution that provides 24×7 availability of directory services.

(e) Design and use a meta-data schema together with a taxonomy that prescribes what information of the person is registered and in what uniform format and what are the classes of users and their hierarchies. Omission in this regard could lead to a serious confusion in the registration and retrieval processes as the e-government systems scale up to a few thousand users.

Public Key Infrastructure Public Key Infrastructure (PKI) is a more advanced system that not only contains an Identity Management System but also the features of the other two systems, viz. Access Management System and Interaction Management System.

[4]Put an end to an activity

Access Management Systems

An Access Management System serves the following objectives:

- It enables ICT systems to identify the user uniquely by matching the password, digital identity token or other device that carries the digital identity of the user with that registered in the system.
- It authorizes the user to perform only those tasks and transactions that are predefined as per the privileges granted by the system administrator at the time of registration or subsequently.
- It can maintain intelligence of users who try unauthorized access of tasks for which they are not privileged. This would be available to the management for review and remedy.

Access Control Lists (ACLs) and *Advanced Access Control Lists* are industry standards in this area.

Interaction Management Systems

The objectives of interaction management are by far the most comprehensive and complex. They include assurance of the following principles of a comprehensive security, which are, in a way, the founding pillars of interaction management.

Authentication Authentication or the assurance that the user is actually the person who s(he) claims to be.

Integrity Integrity or the assurance that the message or document sent or transaction effected[5] through an ICT system has not been tampered with, traveled from to destination safely and got stored therein securely.

Confidentiality Confidentiality or the assurance that the content of the message or document sent or transaction effected has not been read by anyone else except the person to whom it has been sent.

[5]Settled securely and unconditionally

Non-repudiation Non-repudiation or the assurance that the person who has transacted shall not repudiate the same at a later date.

The above four axioms are fundamental to a secure digital environment and flourishing of e-government transactions. These are more significant for the e-government scenario because these four requisites are precisely needed for a whole gamut[6] of e-government transactions involving exchange of contracts, title deeds, issue of statutory certificates, financial transactions, filing of tax returns, approvals and sanctions accorded through a work-flow, etc. PKI is a mechanism that gives all the four assurances.

Tools for User Management

Username and Password system Username and Password system is the conventional system of user management. It has several security issues. The user can compromise the password. The password can be hacked. The password can be transferred. It does not assure that the person keying in the password is the real-world person to whom it was assigned.

Digital identity token A digital identity token is a popularly used device to overcome some shortcomings of a simple password. It is a photo ID card that also has the password embedded in it either magnetically or as a chip. It serves the dual purpose of controlling the physical access to the work premises and of controlling access to the ICT systems that the user is authorized to access. It is quite suitable for employees in corporate work environments. The digital identity token is not completely foolproof or transfer-proof because it depends on human intervention at the entry point through verification of the photo ID with the person's face.

Biometric device A biometric device seeks to overcome the deficiencies of a token by using the physical features of a person, such as the fingerprint or iris to establish identity uniquely. These features are captured at the time of registration, converted into a code using certain algorithms and stored for comparison at the time of authentication.

Public Key Infrastructure (PKI) Public Key Infrastructure (PKI) is a technology that is based on the theory of cryptography or converting an intelligible text or digital content into a form that can be decrypted and read by the user or person to whom it is sent. PKI basically uses the concepts of

[6] A complete extent or range

Digital Signature Certificate, *Asymmetric Key Pair*, *Public Key*, *Private Key*, Digital Signature and Encryption.

Digital signature certificate A digital signature certificate is a document issued by Certification Authority (CA), legally clothed with powers to do so, to a person, creating the digital identity of that person after satisfying that the person truly is who s(he) claims to be. The CA may employ a number of Registration Authorities (RAs) for conducting such verification and front ending the process of issuing digital signature certificates. The digital signature certificate also contains the *public key* of the person, besides details like name, address, and date of validity of the certificate. The CA can revoke a digital signature certificate in case it is no longer required or the user violates the conditions of the certificate, such as compromising the *private keys*.

Asymmetric key pair An asymmetric key pair is a set of two complimentary keys or codes, generated using an algorithm such that:

(a) a text, document or message encrypted using one key can be decrypted only by the other key, and

(b) it is not possible to derive one key from the other.

Public key A public key is that part of an asymmetric key pair that is displayed or published for information and usage by public. It is a part of the PKI directory. The public key of a person is used by others to send an encrypted message to that person. The public key of a person is also used by the recipient of a message or document in verifying the digital signature of a person attached to a message or document.

Private key A private key conversely is the second of the key pair that is to be retained and stored confidentially by the holder of the digital certificate. The private key is used by a person.

(a) to decrypt messages sent by others (using his or her public key), and

(b) to digitally sign a message or document.

PKI, if implemented as part of a comprehensive security policy, can meet the requirements of authentication, integrity, confidentiality and non-repudiation.

Setting up of PKI in a country involves the following steps:

Step 1: Enacting legislation required to give legal status to electronic transactions conducted in conjunction with PKI.

Step 2: Selection of agencies in the public and private sectors, which can be licensed to set up the required infrastructure and act as CAs, after conducting an audit of their capabilities and track record.

Step 3: Promoting the use of PKI for e-government, by taking up specific initiatives in the areas of taxation, customs clearances, land titles and such high-value, high-stake areas.

Step 4: Notifying the designated official or group within the agencies piloting the PKI within e-government as RAs.

Step 5: Perhaps, as may be required initially, to subsidize the cost of digital certificates to promote the concept, as otherwise, the cost of a certificate could be prohibitive at low volumes.

Example of PKI: *RSA Security*.

5.3.2 Transport Environment

Transport Environment includes all the space between the users internal and external and the ICT assets of the e-government system. The need for maintaining the authenticity, integrity and confidentiality of the information is as important here from the security point of view as in the other two environments. Transport Environment is also one over which the administrators of the e-government systems do not have a total control—physical or electronic.

Transport Environment consists of the LANs, WANs, wireless and RF networks, satellite-based networks (VSAT) besides the Internet, which is a critical component the transport infrastructure. All the networks except the Internet can be secured through appropriate means, within the control of the administrators. There are *three* popular ways of tackling the security issues arising out of the use of Internet:

- Creating a Virtual Private Network (VPN) in the public domain
- Installing firewalls at each interface point between the Internet and the agency networks and
- Encrypting the data communicated over the Internet.

Virtual Private Network (VPN)

VPN is a secure network over an insecure network. VPN technology involves creation of a secure, 'private' network—or a tunnel—in a public network to provide secure communications. VPNs provide confidentiality by encrypting data sent over it. They provide integrity by using *checksums* to ensure packets are not corrupt. VPNs verify the identity of the sender before establishing the connection with the agency intranet. They also have features that support access management and non-repudiation.

The benefits of VPN include cost savings, security that is better than in a purely Internet-based communication channel and enable remote access of ICT resources without a dedicated connection.

VPN technology involves three components — a *VPN client* software, a *VPN gateway* at the entry point of the agency or enterprise and a *VPN management application* that ensures the features of PKI are integrated. IPSec (Internet Protocol Security) is the protocol most commonly used in creating VPNs. At the client end, IPSec encrypts the data packets, encapsulates them in an ESP (Encapsulating Security Payload), which is then enclosed in an IP packet and transported. The process of 'unpacketing' and decrypting happens at the VPN gateway.

VPN is not an unmixed blessing. There are issues such as the following:

1. The payload of security in encryption and decryption is heavy
2. There are performance and QoS issues
3. Prone to Denial of Service Attacks
4. Scalability issues
5. Management issues, especially those relating to client side

VPNs for e-Government *e-government often involves establishing a secure connectivity between the HQs of various agencies and its remote field agencies, to support enterprise-wide applications. Establishing dedicated networks involves expense and time much beyond permissible limits. In such circumstances, VPN can be evaluated as a viable option.*

5.3.3 ICT Assets Environment

ICT assets are by far the most valuable and sensitive from the point of the enterprise. The hardware, the software, databases and knowledge is held centrally in the conventional EDP winds or in data centers. As shown in

Table 5.1, two broad categories of security treatments are required here—the *physical security* and *electronic security*.

5.3.3.1 Physical Security

Physical security involves steps that guard against physical damage or loss, These steps include:

1. Aggregation of the core ICT assets in highly guarded data centers, with restricted entry through biometric-controlled doors.
2. Provision of dust-proof air-conditioned environment in the data centers, preferably built to industry standards, with raised floor, special cabling for power and communications, fire protection systems, alarms and closed-circuit TV monitoring of the premises, etc.
3. Discouraging or prohibiting the use of USBs that are likely to infect the systems with viruses.
4. Prohibiting the use of the assets of the system for personal e-mail and browsing.
5. Providing fail-over and redundant systems to ensure 24×7 availability and eliminating single points of failure.
6. Rigorous and automated systems of backup and archival.
7. Maintenance of audit logs and their review.
8. Deployment of biometric-controlled access to workstations and applications.
9. Provision of high quality UPS systems for guarding against power fluctuations and outages.
10. Above all, mirroring of the core data and applications in a remote Disaster Management site.

5.3.3.2 Electronic Security

Electronic security involves placing controls at all the digital entry and exit points to monitor the digital traffic that enters and goes out of the enterprise. The electronic security tools broadly fall under three categories:

- Anti-virus systems
- Firewalls
- Intruder detection systems

5.3.3.2.1 Anti-virus systems A computer virus is a malicious software program that is capable of attaching itself to executable files, data, hard disks or to removable disks and can execute itself repeatedly, replicate itself several times or propagate itself over networks without the knowledge or permission of the user. Such repeated execution, replication or propagation may have the dangerous effects, such as the following, in increasing degree of damage to the host system.

- Occupying valuable disk space
- Slowing down of the system due to excessive consumption of the memory capacity
- Slowing down or clogging of networks
- Corruption of data residing on hard disks and other media
- Corruption and the consequent dysfunction of the application programs
- Infecting the other computer systems that the user's system communicates with.

Virus programs are written and propagated by their authors purely with malicious intentions of causing inconvenience or damage to the targeted users or to the community of computer users at large. The virus programs are also called *malware*. Virus programs are the instruments of cyber-terrorism and pose an unknown but serious threat to the security of all computer systems. The computer community has to guard itself of the dangers posed by the virus menace[7] appropriately to protect the ICT assets and to provide information and services in a reliable manner to the customers and to continue internal operations without a break.

The other broad categories of malware programs are *worms* and *Trojan horses.*

Worms are parasitic computer programs that replicate themselves without infecting other computer files, either on the user's computer or in the other systems to which the user is connected over a network.

A *Trojan horse* is a computer program that pretends to be a harmless program but actually executes certain actions that the user does not expect to do. It is not a virus in the strict sense as it does not replicate itself.

[7] threat

Types of viruses Computer viruses are as variant, stubborn and painful as their biological counterparts. It is essential to know these broad categories to be wary of the possible consequences and take preventive security measures.

Boot sector virus *Boot Sector Infector (BSI)* is a virus that gets access to and resides in the boot sector or the area of the computer (usually on the hard disk) where the initial programs required to start a computer are stored. Whenever the computer tries to read the boot program, the virus gets into the memory and executes itself to gain control over all the computer operations. It can infect all the files and also propagate over the network fast. It is quite a nasty species as it poses immense problems to get rid of.

Macro virus A malicious program written in macro language (a language used to conduct repetitive tasks in a computer product, e.g. MS Word or Excel) that attaches itself usually to Word documents and does its damage whenever the document is Opened It also spreads to other document files. It can be highly annoying.

Encrypted virus A virus that propagates in an encrypted manner to escape detection by the anti-virus software. The virus also carries its own decrypting algorithm. Each time it decrypts itself, it produces a different code that can cause the intended damage to the system. By virtue of the unpredictable sequence of the decrypted code, the encrypted virus escapes detection. Variants of the encrypted virus are the:

- *Polymorphic virus* (which creates varied versions of itself, but containing its original potential to damage),
- *Mutating virus* (which mutates or changes as it progresses through its course in the host system),
- *Self-encrypting virus* (which encrypts its signature code differently each time it infects),
- *Self-garbling virus* (which garbles its code when it is in transmission, but 'degarbles' itself when the host program has infected runs) and
- *Stealth virus* (which intercepts the disk access requests made by the anti-virus programs and feeds them a clean image of the infected file to indicate the file size as it was before infection).

All these categories of viruses are intended to deceive the anti-virus software, conceal themselves in different ways, escape detection and proliferate[8].

Anti-antivirus viruses These are virus programs that infect and disable specific anti-virus programs installed on a system and thereby continue their damage.

Antivirus virus These are viruses that specifically look for and remove other viruses.

Relevance of anti-virus software to e-government Securing e-government systems from viruses is extremely important for the following reasons:

- *Availability* of e-services on a 24×7 basis is a requisite. e-government systems cannot be shut down for disinfection as it would adversely affect the reliability.
- *Trust and confidence* of the citizens would be shattered if the valuable transactions recorded by them in e-government systems get corrupted or obliterated[9] due to virus attack.
- Several *sensitive* functions would be seriously affected in the event of a virus attack.
- e-Government systems have special *vulnerability* from the point of view attacks by authors of viruses.

Anti-virus techniques

Prevention Agencies and enterprises should have rigid and clear virus prevention policy as part of their overall security policy. It should lay down severe restrictions on the usage of USBs, downloading pirated games or games and programs from untrusted sites and other potentially virus-carrier programs, send timely alerts to all users against opening e-mail suspected to carry virus, and do regular scanning of all systems and so on.

Protection Defense in depth and an integrated solution are recommended practices in virus protection. The defense in depth method involves appropriate steps and solutions at three levels, namely, the *user level*, the *backend systems level* and *perimeter level*.

[8]Grow rapidly
[9]Reduced to nothingness

5.3.3.3 Intrusion Detection Systems

Intrusion Detection Systems (IDS) are automated monitoring systems that watch for abnormal, unauthorized or malicious activities. The role of IDS is to watch the traffic patterns, analyze traffic content, review the firewall log files and monitor user account activity. IDS can warn system administrators when an attack or intrusion is taking place.

Depending on the sophistication of the IDS, it can be configured to repel attacks on the fly or track down the origin of the attack. It is not strictly required to protect the network from Internet-based attacks, but it does provide a more extensive and automated monitoring system. Repeated unsuccessful attempts to access the systems, accessing the systems apparently by registered users but at unexpected hours or from different locations, unprecedented high volume of traffic coming from a particular source, etc. are enough reasons for the IDS to suspect a security breach and to alert the administrators.

5.3.3.4 Firewalls

Firewall is a computer system or a group of systems hardware and software that an access control policy between two separate networks, such as between two LANs or two WANs or a LAN and a WAN or most usually between a LAN/WAN and the Internet. The key feature about a firewall is that is only a mechanism to enforce the access control policy of the agency. The prerequisite for the successful deployment of a firewall, therefore, is the design and promulgation of an enterprise security policy. Firewall serves the basic purpose of making it nearly impossible for unauthorized users to access the ICT assets (situated 'behind' the firewall) while permitting the authorized users to access the same effortlessly.

Firewalls typically adopt the following techniques for the 'inspection' required for implementing the security regime. An understanding of these techniques enables e-government managers to better manage the security policy.

Packet filtering The firewall filters the IP packets with reference to the do's and don'ts or security rules prescribed by the organization. It validates the intelligence it gathers from each packet against such rules.

Network Address Translation (NAT) Firewalls also translate or replace the internal or private IP numbers assigned to systems within the network with its own public IP address so that the individual systems within

the LAN of the enterprise are not visible to the outside world and are more secure to that extent.

Application proxy or proxy server A firewall can also act as a proxy of the systems within the network, when such systems want to interact with the outside world for such services as e-mail, Internet access, file transfer, etc. A proxy server acts as a buffer between the internal workstations and the Internet.

Logging and monitoring Firewalls have features that keep a record of the events that happen within its purview. All exceptional or abnormal events are so logged, for review by the security administrators. In the event of a high risk anticipated at the firewall, it is programmed to send appropriate alerts to the security administrators for prompt remedial action. For instance, when the firewall suspects a 'sniffing' or pre-attack surveillance by an outsider, it sends such an alert.

Content filtering Firewalls use the technique of content filtering to block objectionable sites being accessed by the users or messages containing predefined objectionable or obscene words being sent out of the system or received into it.

5.3.3.4.1 Types of Firewalls Firewalls are basically of two types: *hardware firewalls* and *software firewalls*.

Hardware Firewalls These are security appliances that contain the hardware and software bundled into one. The firewall software is preloaded into the appropriately sized hardware and configured for optimum performance with the result that the setup is quite quick. Hardware firewalls are the preferred option when an organization wants to put in place a security system quickly following a serious attack. Hardware firewalls tend to be more expensive and less flexible as compared to software firewalls.

Software firewalls These are software packages that need to be installed on the existing hardware of the enterprise or hardware procured separately for the purpose. Due to the availability of a wide range of software firewall products in the market, this would be a preferred solution when the security needs of the agency are specific. Software firewalls are less expensive, but require more time for installation and user training. There are also personal firewalls for free download, which are suitable for standalone PCs.

5.4 e-Government Security Architecture

Security Architecture is a high level document that directs and guides the security efforts of individual e-Government initiatives and projects setting out the security objectives and goals, prescribing the standards to be achieved and indicating the procedures and processes that need to be followed by all the players participating in e-government, users, citizens, businesses, e-government partners, operators and service providers.

The goals of the security architecture are to:

- Create the necessary levels of confidence and trust among the stakeholders-citizens, businesses and government users.
- Enforce global standards of security practice and implementation in e-Government.
- Create and enforce digital identities including registration and enrollment as a means of accessing electronic government services.
- Strengthen the four pillars of security i. e. *authentication*, *integrity*, *confidentiality* and *non-repudiation*.
- Enhance the security awareness among the users through dissemination of a set of security guidelines.
- Promote the development of operational schemes called security policies by individual government agencies.

Security architecture seeks to achieve the above objectives by addressing the regulatory, technological and managerial issues arising out of the security needs and requirements of

- user environment
- transport environment
- ICT assets environment.

The security architecture, usually accompanied by a set of security guidelines, contains the following:

- A description of the security environment consisting of the three portions mentioned above and what the e-government assets are the need to be secured and what the perceived security threats are.
- A description of the security requirements in functional and technical terms.

Any national or state government, intending to take up an e-government initiative seriously, should design an appropriate Security Architecture and Framework as a first step. This sets up the security vision in clear terms.

The formulation of a Security Architecture and Framework has to be quickly followed by three more initiatives:

- Providing a *statutory basis* for the e-government security architecture and mandating the security requirements on agencies that are partners in e-Government.
- Defining *security standards* to be followed.
- Encouraging individual agencies in the public and private sectors to design appropriate *security policies* that give a concrete shape to the manner of implementing the architecture in specific relation to the particular agency or enterprise.

5.5 Security Standards

The standards for information security was set up by the *British Standard BS 7799*, which on account of its immense popularity was adopted by the ISO as *IS0 17799*. There is also a sequel *BS 7799-2* that prescribes the specification for Information Security Management.

The versions of these security standards are *ISO/IEC 17799*, which is the Code of practice for Information Security Management, and *BS7799-2:2002* which gives the Specification for Information Security Management.

ISO/IEC 1799 is a standard that sets out the requirements for an Information Security Management. It helps identify, manage and minimize the range of threats to which information is regularly subjected. It defines 127 security controls structured under 10 major headings to enable the IS managers to identify the particular safeguards that are appropriate to their particular business or specific area of responsibility.

BS7799-2:2002 tells us how to apply *ISO/IEC* 17799 and how to build, operate, maintain and improve an ISMS.

The 10 major security areas identified by *ISO/IEC 1799* and the ISMS methodology of implementing the security are mentioned briefly below, as they are central to an e-Government security policy.

5.5.1 Ten Controls Prescribed By ISO/IEC 17799

1. *Security policy*: Provides management direction and support for information security.

2. *Personal security*: Reduces the risks of human error, theft, fraud or misuse of facilities.
3. *Access control*: Secures management of access to information.
4. *Compliance*: Avoids breaches of any criminal and civil law, statutory, regulatory or contractual obligations, and any security requirement.
5. *Systems development and maintenance*: Ensures that security is built into information systems at the design and development stage.
6. *Communications and operations management*: Ensures the correct and secure operation of information communication and processing facilities.
7. *Organization of assets and resources*: Helps manage information security within the organization.
8. *Asset classification and control*: Helps identify assets and protect them appropriately.
9. *Physical and environmental security*: Prevents unauthorized access, damage and interference to business premises and information.
10. *Business continuity management*: Avoids interruptions to business activities and protects critical business processes from the effects of major failures or disasters.

We can see that

- the first five controls relate to the user environment
- the sixth one to transport environment and
- the remaining four to the ICT assets environment.

5.5.2 Information Security Management System (ISMS)

The information Security Management System (ISMS), also called Information Security Policy, is a document prepared by a government or an agency and addresses the following questions:

- Why is information security important in the context of the e-government program or initiative?

- What are the threats perceived to be important? What are the possible attacks? What is the level of risk that the agency can accept or tolerate?
- What are the environments that we want to protect? In other words, who are the users, what are the communication channels, and what are the ICT assets that we want to protect? List, identify and classify them.
- What are the roles and privileges that we want to give to the users of various categories? Who is allowed to do what? What is the policy of the enterprise for e-mail, chat, web access, system administration, development and maintenance?
- How do we want to treat or manage the risks identified with the controls selected? In other words, what tools do we intend using for treatment of risks?
- What are the organizational arrangement that ensure management of the security policy and its continuous review and audit?

The ISMS of Information Security Policy is a working document that guides, instructs and canalizes the actions and efforts of all users of the ICT systems. Figure 5.2, adopted from the Standard, defines a PDCA or Plan-Do-Check-Act cycle for management of the security.

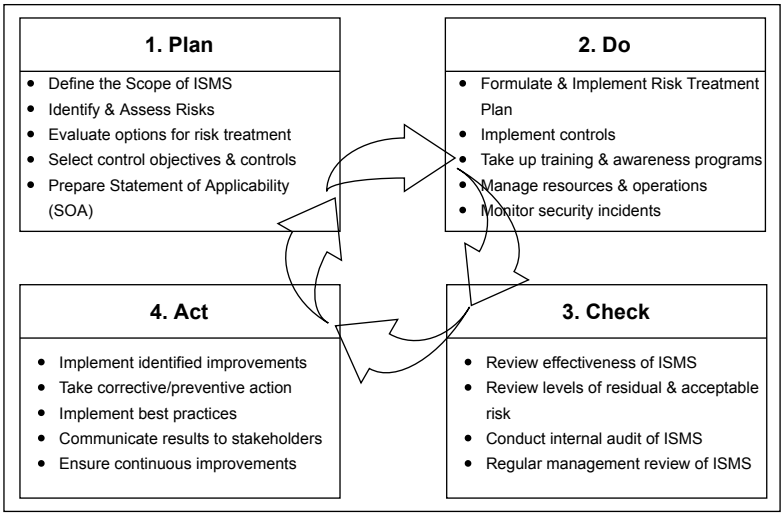


Figure 5.2: The PDCA Model of Security Management.

Information Security is quite critical to the success of e-Government. We need a comprehensive security approach that spans across the user, transport and ICT assets environments. Publication of an e-government security architecture and preparation of an Information Security Management System, in conformity with the international standards are the most desirable practices.

CHAPTER

6

MANAGING E-GOVERNMENT

Management of e-Government implementation involves the following:

- people
- process
- technology
- finance and
- partnerships

Managing People

e-Government has to be designed, developed, delivered and used by people — people within government agencies, people outside the government in organizations that government would have to partner, citizens and business people. People management involves the following:

- Awareness building
- Education
- Training
- Coordination
- Team building
- Development of leadership qualities

Managing Process

- **Service definition**: e-Government is about being service-centric.
- **BPR (Business Process Re-engineering)**
- **Legal process reform**
- **Delivery channel reform**

Managing Technology

- **Design and development of architectures**
- **Prescription of standards**
- **Security**
- **Procurement**

Financing e-Government Projects

We need experts who can find innovative methods of financing e-government projects.

Managing Partnerships

- **Designing suitable partnership models**
- **Crafting the contracts**
- **Steering the partnerships**

6.1 Approaches to Management of e-Government Systems

There are different ways in which management for e-government can be understood. Three possible approaches to e-government responsibilities (see Figure 6.1):

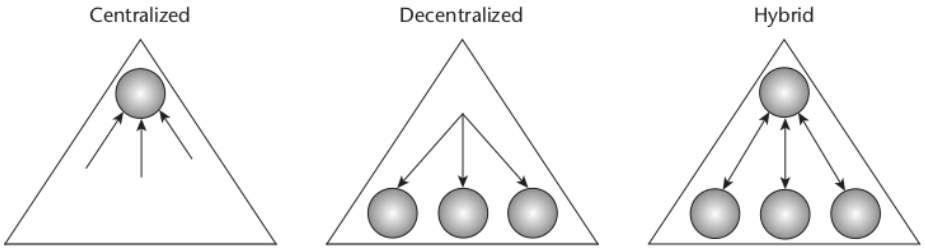


Figure 6.1: Different approaches to e-government systems responsibilities

1. **Centralized**: Decisions are taken at the most senior or central level.
2. **Decentralized**: Decisions are taken at some level lower than the most senior; typically by individual work units within the organization or even by individual staff. The latter may also be referred to as end-user computing, where the individuals within the public sector who make use of outputs from e-government systems (the internal end users) are also those who operate and/or develop and/or manage those systems.
3. **Hybrid**: Decisions are taken at both senior and lower levels, either separately or in an integrated manner. This approach is called federal or federated in some governments.

6.1.1 Centralized Approach to e-Government

Some examples can be given of what a centralized approach to e-government would mean. In terms of computing and data management architecture, a centralized computing architecture would be one which involves a large central computer with dumb terminals or network computers attached. That represents an internal view of architecture. An external view sees centralized data architecture in terms of portals: single central web locations through which all data is routed to users.

Under a centralized approach, e-government systems are typically developed by a team from the central IT unit, or by external contractors under central IT unit control. The content and timing of individual projects can be drawn from any e-government strategy that has been developed. That strategy could also be used to guide procurement, where organization-wide standards would be set for hardware, software and telecommunications equipment. Typically, a central group is responsible for setting standards, arranging contracts with suppliers, policing standards, and giving final approval on all IT purchase requests. Purchases of IT and IT budgets are routed through a central control point.

In a centralized approach, training is planned and prioritized organization-wide to fit in with e-government plans. Like technical support, it may be delivered by external providers or by specialist staff from the central IT unit.

6.1.1.1 Benefits of a Centralized Approach

Achievement of scale economies Centralized approaches allow most activities to be undertaken more cheaply per unit. Items purchased externally — computers, software packages, consumables, staff training, systems development, consulting, and so on — can be decided upon once and then bought in greater bulk. Activities undertaken internally — from system development to implementation and maintenance, and management of all these processes — cover a greater number of staff.

Avoidance of duplication One main intention of centralized approaches is to have a single version of any particular e-government system for the whole organization, and to store any item of data once and only once. As a result, there is no wasted effort, no wasted storage capacity, and no inconsistency of data. For example, only one accounting application needs to be developed for the whole agency. Similarly, if dealing with a set of external clients (such as businesses), each client's name and details are captured once for use on a single, shared database. If these details change or if the required data structure changes, only one set of amendments needs to be made. The database represents the single authoritative source of digital information in the organization. This saves money, and can also improve data quality.

Sharing resources A well-planned centralized system holds data used across the organization in one place, allowing all staff to access it. This makes it cheaper, faster and easier to undertake organization wide activities. Central planning and operation also allows compatible technology and skills to be introduced. Exchange of hardware, software and staff between organizational systems and units therefore becomes much easier and less costly.

6.1.1.2 Disadvantages of Centralized Approaches

Heavy time consumption Centralized decisions and actions can be more time-consuming than for a decentralized approach because of:

- the additional time it takes for information to flow up the organization as an input to centralized decisions;

- the additional time it takes to collate information from a variety of different decentralized locations as an input to centralized decisions; and
- the additional time it takes for implementation information to flow down the organization.

Limited ability to meet user needs Centralized approaches necessarily mean that priority goes to those e-government systems which are seen as important by some select and centralized staff group. The priorities of the periphery – both individuals and individual work units inside government, as well as clients outside government may not be addressed.

Inflexibility The greater the amount of central planning that has gone into an e-government system decision, and the longer that decision is therefore intended to provide guidance for the organization, the less flexibility it offers the organization to cope with differences between local units, or with internal or external changes.

6.1.2 Decentralized Approach to e-Government

Examples of a decentralized approach to managing e-government systems responsibilities can be provided. In terms of computing and data management architecture, a truly decentralized computing architecture would be one that involves standalone computers or, possibly, a peer-to-peer network. Decentralized approaches are commonly associated with the spread of personal computers throughout an organization. An external view would see multiple websites and other routes through which data could be accessed.

Under a fully decentralized approach, e-government systems would be developed within organizational work groups, focused on their requirements, or even by individual end users. Decentralized procurement means that individuals or groups select and procure whichever technology best suits their particular needs. Similarly, a decentralized approach to training means that individuals or small groups plan their own training needs. It is likely that training takes place on the job or through informal coaching of one staff member by another.

6.1.2.1 Benefits of Decentralized Approach

Greater fit between systems and local needs The closer the proximity of user and developer, the less the communication gap and the more likely it

is that the developed system meets the users' real needs.

Faster system development The less the organizational distance between system user and system developer, the faster development of that system is likely to be.

Perceived lower costs Decentralized approaches present lower costs than centralized approaches in certain areas. This is thanks to:

- faster development,
- less miscommunication,
- greater fit to local needs through smaller design–reality gaps,
- the greater emphasis on smaller computers,
- the greater emphasis on buying software packages rather than developing software in-house, and so on.

6.1.2.2 Disadvantages of Decentralized Approach

Barriers to sharing data Decentralized approaches can create e-government systems in different work units that are mutually incompatible.

Barriers to sharing other resources, including human resources There may also be an inability to share other resources if work units are allowed to set up their own separate e-government systems. It may be hard to exchange hardware and software. Perhaps more importantly, each individual system requires a unique set of skills for system development, implementation and operation. This makes it more difficult for staff to move between different e-government systems.

Duplication of effort Decentralized approaches also tend to be very costly because units will often duplicate what others are doing.

Duplication covers analysis, design and implementation of e-government systems; gathering and administration of data; and system operation, support and maintenance.

This imposes extra costs in gathering, maintaining and updating data.

Lack of learning and control In addition to the extra direct costs that duplication imposes, there is an indirect cost of lost learning opportunities and limited cross-fertilization of ideas.

6.1.3 Hybrid Approach to e-Government

Both the centralized and the decentralized approach to managing e-government can provide benefits for public organizations. Yet, at the same time, such approaches can be hard or impossible to implement, and can produce serious disadvantages for the organization.

What is the way out of this quandary?

One way forward is the adoption of a hybrid approach that attempts to reconcile the push of the centralized approach with the pull of the decentralized approach.

A hybrid approach to e-government can be feasible and provide distinct benefits. A decentralized approach may be most economic for public organizations, because it saves on overt input costs. A centralized approach may be most efficient, because it avoids waste and duplication. But a successful hybrid approach may be most effective because it can simultaneously provide:

- the control necessary to share key resources (including data), to avoid duplication, and to achieve economies of scale; and
- the freedom necessary to meet user needs, and to overcome blocks to IT usage and system development.

Examples

Computing and Data management architecture The most common hybrid computing architecture is the client/server model, in which computing power is divided between the central servers and the local client workstations. This architecture has now been adopted by vast numbers of public sector organizations worldwide.

A similar hybrid approach to portals creates a single main portal which merely links through to an existing set of sub-portals.

Systems development A hybrid approach to systems development can involve a division of responsibilities; for example, defining certain types of e-government system as suitable for central development, and others as suitable for decentralized/end-user development.

Procurement Standards for procurement bring many immediate and obvious benefits to public agencies.

6.2 e-Government Strategy

An e-government strategy is a plan for e-government systems and their supporting infrastructure which maximizes the ability of management to achieve organizational objectives. Increasing numbers of public agencies are developing an e-government strategy.

Strategic Planning

A set of core questions about e-government strategy for public agencies are:

Why?

Why are increasing numbers of public agencies trying to develop an e-government strategy?

Following could be the explanations.

- The fad/'me too' factor of copying current trends or copying appearances in other organizations.
- The desire of some senior officials to wrest control of e-government from technical staff and/or individual departments.
- The desire for the kudos[1] and resources associated with a major organizational initiative.
- The demand for such strategies from central government agencies.

In addition, the growth of e-government strategies in the public sector is impelled by the potential benefits that a strategy can bring.

Some of these are political, such as:

- providing senior management control over organizational systems,
- accessing central funds that are only available on production of a strategy, and
- avoiding public reprimands and penalties where strategies are demanded by higher level bodies.

An e-government strategy is also seen as a key mechanism to produce centralized approach benefits

Finally,

[1] An expression of approval and commendation

- a successful strategy can develop senior management understanding that e-government systems are information systems not just IT.
- It permits a fundamental review of the organization's use of information and technology, leading to a comprehensive understanding of information systems requirements.
- It also provides a detailed plan of action on e-government for the organization.

What?

Like any strategic plan, an e-government strategy seeks to answer three questions, illustrated in Figure 6.2:

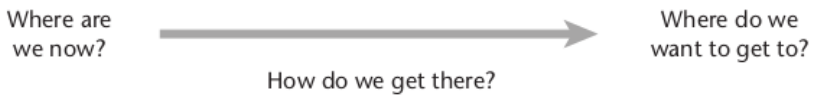


Figure 6.2: Overview of strategic planning

- **Where are we now?** (i. e.how are systems working now, and what external factors affect them).
- **Where do we want to get to?** (i. e. in the future, how should the organization's e-government systems be or work differently from at present).
- **How do we get there?** (i. e. what actions need to be undertaken to achieve the outcome identified in answering the second question).

When?

In simple terms, the answer is: 'You undertake e-government strategy when the time is right'.

In other cases, we undertake e-government strategy when:

- e-government systems being created without consideration for overall organizational objectives;
- outdated systems still in use due to inability to plan alternatives;
- data that cannot be shared between different e-government systems because there are no organization-wide standards;

- IT being seen as the end rather than the means; in other words, when e-government is seen as an end in itself;
- no clear locus of responsibility for dealing with these problems;
- comparative organizations have a strategy.

6.2.1 Steps of e-Government Strategic Planning

eGovernment strategic planning is typically conceived as a series of steps that are undertaken systematically over a period of a few weeks or a few months. These steps are summarized in Figure 6.3. Once completed, they produce a framework for organizational action that can endure for a number of years.

Step 1: Create e-government planning structures/roles

Step 2:
a. Audit information systems
b. Get guidance from organizational strategy

Step 3: Set e-government objectives and principles

Step 4:
a. Determine e-government systems architecture
b. Determine e-government organizational architecture

Step 5: Disseminate and plan e-government actions

Step 6: Manage, evolve and review e-government strategy

6.2.1.1 Strategy Foundation: Create eGovernment Planning Structures/Roles

- In order to control the process of strategic planning, a special body is usually set up, called something like 'eGovernment Steering Group'.
- It will typically consist of senior staff or other powerful stakeholders from various parts of the organization, together with some technical advisors.
- this committee is likely to be chaired by a Chief Information Officer (CIO).

This body normally reports to the very top levels of the organization because of the strategic nature of its work, which includes:

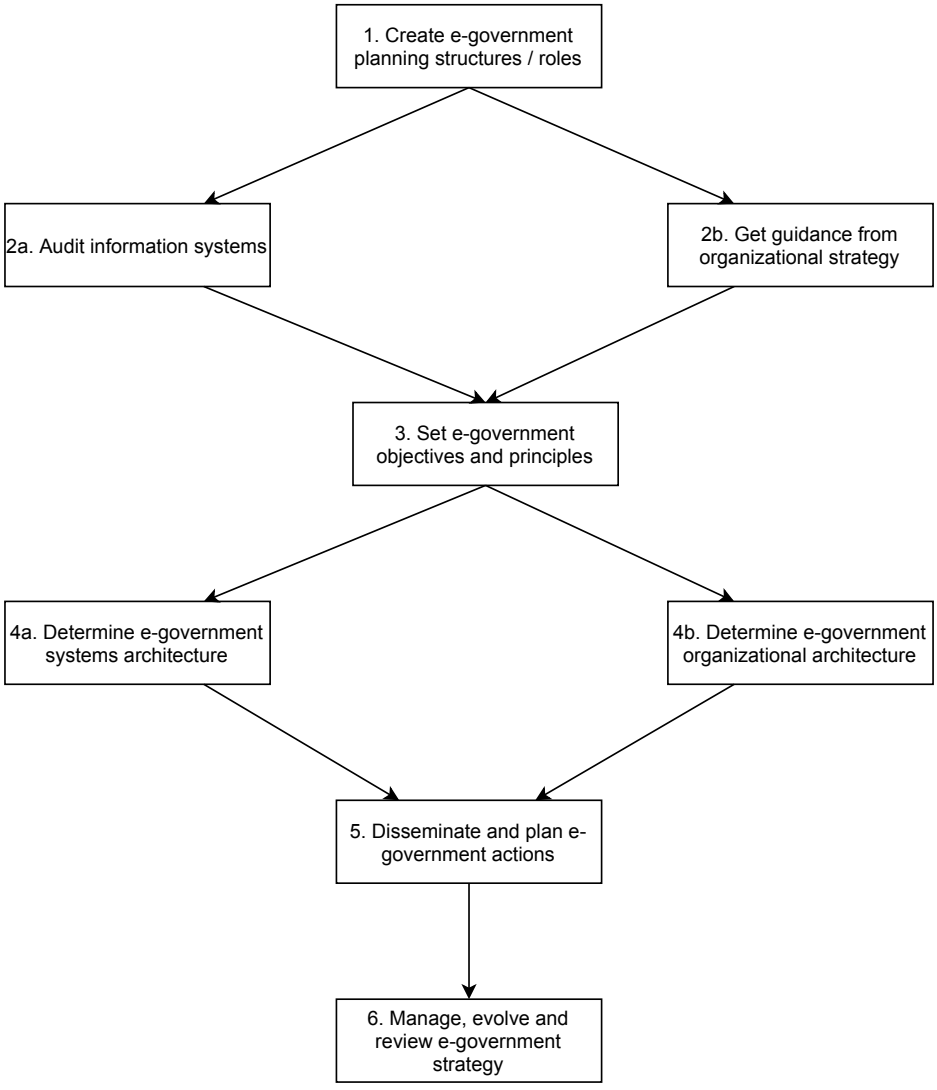


Figure 6.3: The steps of e-government strategic planning

- setting the scope of, and commissioning the e-government strategy;
- taking necessary strategic decisions relating to e-government systems (such as those presented during strategic planning);
- communicating the e-government strategy to the rest of the organization;
- ensuring the necessary resources are in place to achieve strategic objectives, and allocating those resources; and
- monitoring and controlling the overall development and operation of e-government within the organization, and checking this against stated objectives.

6.2.1.2 Strategic Analysis: Audit Information Systems

An e-government-specific answer to the question 'Where are we now?' requires a comprehensive understanding of the current state of e-government and other information systems.

It includes all types of information system, manual or computerized: hence the title 'audit information systems' rather than 'audit e-government'.

Information systems (IS) audit is often conceived in a very narrow sense, just as an inventory of IT within the public agency: all computer applications with their hardware, software, networks, physical location, licensing and ownership; and often just security-related. However such an approach is far too narrow to form an effective analytical base for strategy. It must be expanded in several ways, as below:

Systems perspective Audit must recognize the full information system, describing not just the technology resources, but also:

- the information that information systems deliver,
- the information processes undertaken, and
- the human resources involved,
- covering information skills (e. g. data gathering and presentation), IT skills (e. g. hands-on computing), and system development skills (e. g. systems analysis and design).

Issues perspective The audit should be more than just a list of resources, but should help identify key issues that will inform and affect subsequent decision-making on e-government. These might include a sense of important problems or complaints facing the current information systems, or an assessment of emerging trends.

Contextual perspective This includes the outer two layers of the 'onion-ring' (see Section 1.2) within the audit.

- It will look at management systems and structures within the public agency.
- It will look at IT trends and standards within the local environment.
- It will review financial and other constraints specific to e-government systems change.
- Perhaps most important, it will incorporate an understanding of relevant policies, guidelines and initiatives that impact on e-government.

6.2.1.3 Strategic Analysis: Get Guidance From Organizational Strategy

An e-government strategy should therefore be firmly rooted in one particular element from the organizational context: the wider organizational or business strategy for the whole agency.

Business strategy first asks,

- 'Where are we now?' An answer would include details of the organization's current structure and functions; key client groups; existing problems that need to be addressed; and important current and forthcoming factors – particularly policies and political priorities – within the internal and external environment.
- It next asks, 'Where do we want to get to?' An answer would include details of the organization's objectives, and some vision of the future organization that will enable it to overcome current and forthcoming problems, and to achieve its objectives.
- Finally, it asks, 'How do we get there?' This would be achieved through a statement of management strategy about major changes to organizational structure and functions in order to reach its future vision.

6.2.1.4 Strategy Framework: Set eGovernment Objectives and Principles

The eGovernment Steering Group may use the data gathered so far to produce a broad statement of the role and objectives of information and of e-government within the organization. This statement may be specific (tying e-government to particular organizational objectives) and/or it may be generic (a general statement of information and IT principles).

These objectives and principles can also be used to develop the criteria against which e-government proposals may be evaluated and/or prioritized.

6.2.1.5 Strategy Definition: Determine eGovernment Systems Architecture

eGovernment strategy can be seen as needing to lay out the ITPOSMO dimensions for the future (see Section 1.2) The information, technology and process dimensions are together seen as an *e-government systems architecture*: a plan of the e-government systems that the organization will require in future. This architecture forms a major element of 'Where do we want to get to?' for e-government.

The e-government systems architecture can be described in terms of the individual e-government applications with details of data capture, input, processing, storage and output plus links to decision and action processes (CIP-SODA: see Section 1.2)

It will also consist of a number of different models, including:

Data model

- A data model showing the structure of unified, organization-wide data to which the e-government systems will have access;
- often illustrated using an entity-relationship diagram.

Process model

- A process model showing the key activities of the organization that the e-government systems will either support or undertake;
- often illustrated using a process diagram.

Data/Process model

- A data/process model showing the organization-wide connection between business processes and data entities, and the organization-wide movement of data that e-government systems will enable;
- often illustrated using a data flow diagram.

The e-government systems architecture will also consist of organization-wide models for:

- **IT**, showing how computers will be sized and connected within the organization, and an outline of the software to be used;
- **data management**, showing how data capture, input, processing, storage and output functions will be divided across the IT architecture.

A summary of all the elements within the e-government systems architecture is shown in Figure 6.4.

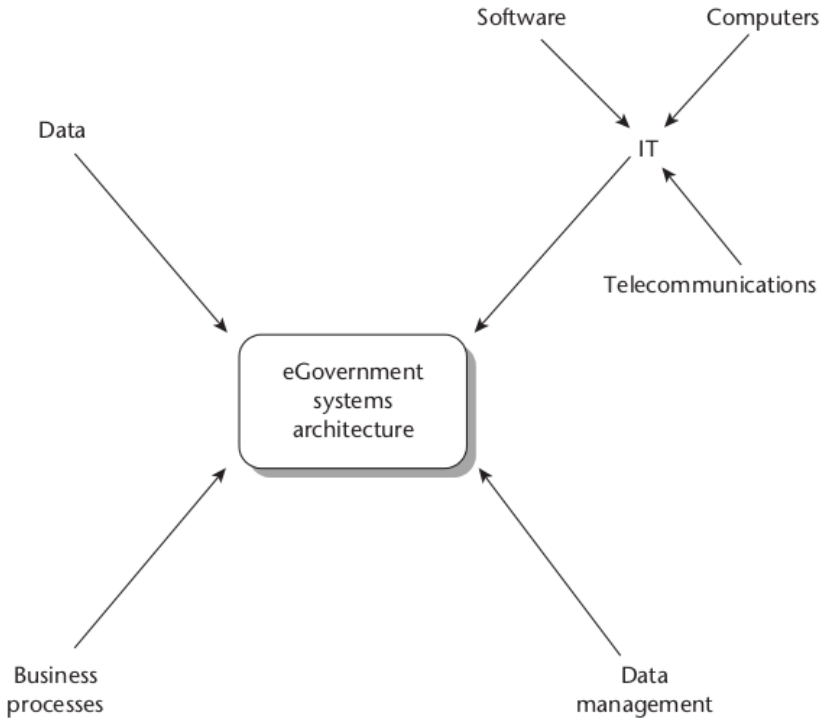


Figure 6.4: Elements of e-government systems architecture

6.2.1.6 Strategy Definition: Determine eGovernment Organizational Architecture

General strategic decisions may include:

- stating the approach to management of organizational change, including a determination of the needs for cultural change;
- clearly allocating responsibilities for e-government systems development and management;
- identifying major competency gaps and approaches to closing them through human resource strategies;
- deciding how back-office procedures may be restructured to support e-government;
- locating the e-government/IT function within the wider organizational structure;
- demarcating which services (e. g. systems development, training and systems operation) are to be sourced in-house and outsourced;
- identifying procedures to be used when tendering for and selecting e-government systems products and services;
- specifying standard systems development methodologies and tools to be used; and
- identifying financial approaches to be adopted, such as public–private partnerships.

6.2.1.7 Strategy Implementation 1: Disseminate and Plan eGovernment Actions

The defined strategy can now be circulated as an 'eGovernment Strategy Statement' and, if appropriate to the organizational culture, discussed and refined.

Once agreed, the strategy is typically planned in more detail in a matrix format.

The columns of the matrix can be a set of e-government project plans, created for improving existing systems and developing new systems. This might include:

- a statement of project objectives;

- an estimation of benefits, risks and constraints; and
- an estimation of resource requirements covering finance, human resources (i. ejobs and skills), technology, and timescales.

The rows of the matrix will be organization wide resource plans:

- for personnel training and development,
- for finance,
- for technology, etc.

6.2.1.8 Strategy Implementation 2: Manage, Evolve and Review eGovernment Strategy

Strategic planning is not intended to be a one-time activity but a continuous cycle that needs to be completely revised at the end of the strategic framework period, or earlier if circumstances change or objectives are not attained.

One task of the eGovernment Steering Group is to monitor implementation of the strategic plan. Monitoring gathers information on:

- performance against objectives set for both e-government overall and individual e-government projects;
- benefits accruing to the organization from e-government systems;
- problems related to developing or operating e-government systems, with diagnoses and proposed remedies;
- other impacts associated with e-government systems;
- changes to significant internal and external factors that affect the performance of the organization; and
- resources used and projected for use

On the basis of the information gathered, the eGovernment Steering Group may decide to modify the strategy.

6.3 Managing Public Data

e-government systems are information systems. The data in e-government systems is therefore fundamental to the functioning of the public sector. It is too easy to assume that all is well with this data. Yet most e-government systems have data quality problems; sometimes so bad that they undermine the whole edifice of government functioning.

We can define data quality in terms of five '**CARTA**' indicators:

1. ***C**ompleteness*

   The degree to which all the data required by users is present in the e-government system.

2. ***A**ccuracy*

   The level of errors/incorrect data within the overall system data.

3. ***R**elevance*

   The degree to which data is necessary in order to complete particular user decisions and actions.

4. ***T**imeliness*

   The degree to which data can be delivered by the e-government system within a required time-frame.

5. ***A**ppropriateness of presentation*

   The degree to which data produced by the e-government system is accessible and intelligible to the recipient.

The more CARTA the data, the higher its quality; the less CARTA the data, the lower its quality.

It is estimated that around higher percentage of system data errors arise during the human elements of the process. Historically, this has occurred mainly during capture and input, because these were traditionally human-intensive tasks with errors arising from misreading, mistyping, and lost or omitted inputs. It has also occurred after output, also because of misreading or misunderstanding.

But data errors can occur at any stage in the information cycle, for example, during processing, storage, output or transmission between those stages, as illustrated in Figure 6.5.

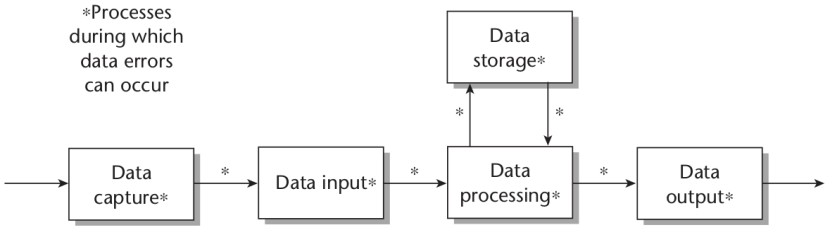


Figure 6.5: Potential data error points in the e-government system cycle

In all cases, the data output will not be accurate or reliable. eGovernment systems with poor data will be prone to collapse as the poor data foundation undermines decision-making and action, as summarized in Figure 6.6.

This is often described as *garbage in, garbage out (GIGO)*: what you get out from your e-government systems can only ever be as good as what you put in, and if you put in garbage, you get out garbage.

This is an issue for all organizations, but it is particularly an issue for the public sector and e-government:

- The public sector is especially information intensive, and therefore relies heavily on data in order to undertake its functions.
- The public sector often has responsibility for decisions that are critical to an individual's, a region's or a nation's welfare.
- The public sector has legal obligations relating to data quality and accessibility, for example in relation to freedom of information.
- It therefore faces a significant threat of litigation if data quality is poor.

The public sector may also face additional constraints — on skills, on technology, related to the large size of its data sets — that increase the risks of data quality problem

6.3.1 Causes of Public Data Problems

We can divide causes into two main camps:

1. **hard**: technical causes of data quality problems and
2. **soft**: human causes.

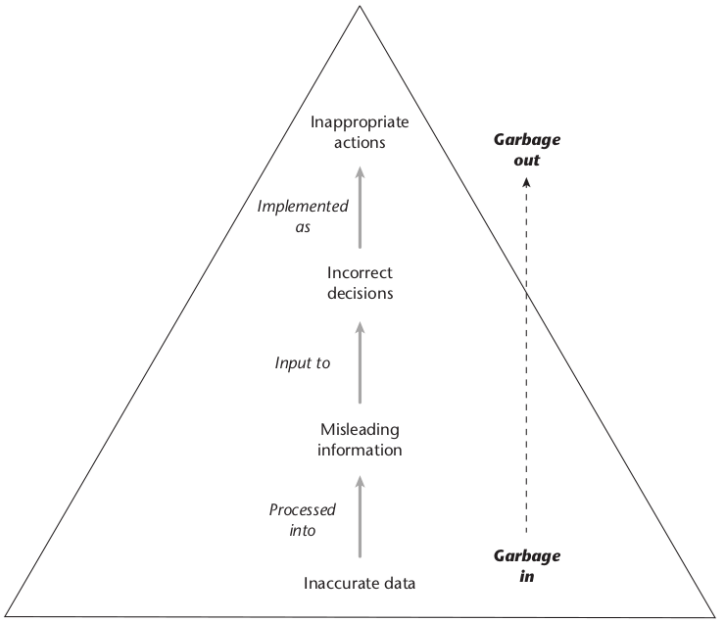


Figure 6.6: Impact of inaccurate data

6.3.1.1 Hard Side: Technical Causes

Looking first at the hard side, one can see that public managers love to blame data glitches on 'computer errors', and that some technical problems do arise which affect the data held by IT:

Environmental hazards

- High temperatures and high humidity can cause hardware components to break down, thus corrupting data.
- Static electricity can damage both electromagnetic components and corrupt data.
- Dust and smoke can short out components and make moving parts stick, especially damaging disk drives and the data on them.
- Fire, flood and lightning have a fairly obvious and catastrophic effect on IT-based systems.

Electrical Problem

- Power spikes or surges (increases in voltage), and brownouts (decreases in voltage) can corrupt disk held data and damage internal components.

- Power cuts cause an ability to work, and a loss of all data in memory.

Equipment breakdown This can prevent data being exchanged or accessed.

Software errors

- The presence of bugs (programming errors) in the software of an e-government system can have any number of effects.
- These include overt or, worse, undetected corruption of data.

But to what extent can these truly be classified as 'computer errors' or technical problems?

6.3.1.2 Soft: Human Causes

The presence of bugs should be seen mainly as a problem of human, rather than technical, origin relating to the management of systems development. Even the actions of environmental or power hazards can often be traced to human inputs in the design, construction or operation of IT-based systems. This must put a question mark over the value of some hard approaches to public data quality.

We can reinforce this point by looking at another way in which technology could be blamed for inducing a further vulnerability and danger to data accuracy: the threat of computer crime.

Computer crime is a major problem for the public sector:

- internally, public employees are a significant source of such crime;
- externally, threats seem to be growing and cyber-security has risen sharply up the agenda in many countries as a result of the terror attacks of the early 21^{st} century.

As well as entry of inaccurate data onto computer systems for personal gain, computer crime also includes:

Alteration of existing data For example, a worker increasing the rate of pay recorded for them in the payroll system, or the defacing.

Unauthorized access to existing data Hackers getting access to critical public data.

Deliberate destruction of data For example, removing part of the organization's financial records just for the hell of it or introducing a computer virus.
Computer crime also covers physical theft of computer hardware or software (software piracy). Some public agencies even include personal use of organizational IT, such as typing and printing a personal letter or buying goods on the web from your office PC.

6.3.1.3 Hard Solutions to Public Data Quality Problems

Hard, technical response to problems of data accuracy, including computer crime requires the imposition of various controls. These can be divided into two groups:

1. **general controls**, which affect all e-government systems; and
2. **application controls**, which relate to one particular e-government system.

General controls

- **Access controls**:
  - Used to control user access to physical or digital components of an e-government system.
  - Examples include security guards and passwords.
- **Communication controls**:
  - Used to control user access over computer networks.
  - Examples include encryption and firewalls.
- **Other technology controls**:
  - Such as controls to address virus, fire or power issues.

Application controls To prevent many kinds of problems, many public agencies use application controls. The most important of these are **input controls**; that is, controls on the process of data entry that can be built into the e-government system. In many cases, if the control is violated, a customized message will appear providing guidance on the problem, and the new record will not be accepted until the error is corrected.

Typically, the controls operate on each field within a database record and are stored as rules associated with that field.

6.3.1.4 Soft Solutions to Public Data Quality Problems

We could identify a different role for each one of the CIPSODA (see Section 1.2) elements of an information system. However, that model can be simplified somewhat to produce the summary shown in Figure 6.7. This removes the roles of storage and output (because technology normally fulfils those roles) and merges the roles of decision maker and actor into the term 'user'.

Figure 6.7: Different data roles played by people in public data systems

The people occupying each one of these roles will have a different perspective on data, and we can develop a simple model of this, shown in Figure 6.8. The model sees perceptions about how data is or is not used as shaping the motivations of each stakeholder which, in turn will shape their actions which, in turn will have an impact on data quality.

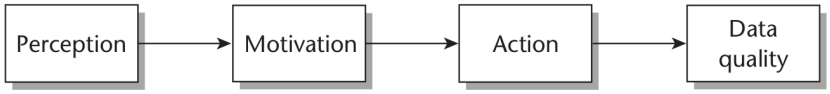


Figure 6.8: A soft perspective on data quality

The soft perspective therefore argues that one of the keys to data quality, or lack of it, lies in the motivations of those involved. Where they are motivated to do so, those involved will help data quality to be high. Where they are motivated to do otherwise, data quality is likely to suffer.

Some examples of perceptions — and their related motivations — will illustrate:

Perception of data irrelevance

- Sources in public data systems, such as those asked to take part in a census or other survey, are often asked to provide data that is for the use of someone other than themselves.
- Similarly, those capturing, entering and processing data are often treated as clerical automata, merely transmitting data to be used by some senior official. In such situations, the humans involved see the data as largely irrelevant to their own work and their own lives, because they never use it.

- As a result, they have limited motivation to worry about data quality, and their actions — for example, lack of care in response, or lack of concern about data entry errors — may undermine data quality.

Perceptions of non-use This is related to the perception of data irrelevance.

- In some e-government systems, those involved know (or believe) that the data they are giving or collecting or inputting or processing is never actually going to be used.
- This will have a knock-on effect on data quality.
- Within the politicized context of the public sector, for example, data entry staff may know that the data they type in is not used; perhaps because senior officials make decisions using informal, political data rather than rational data from the computerized e-government system.
- In that case, perfectly logically, the data entry staff will not be motivated to care about ensuring accuracy of the data they type in.
- Alternatively, take the case of residents asked to provide input to the planning of a community policing strategy.
- Having once taken the trouble to provide data, they might feel that their efforts have produced no discernible result if no sensible strategy emerges.
- Feeling their data was not going to be used they might, in the future, be motivated to refuse to provide further data to the police service.

Perceptions of data-related punishment

- Citizens and businesses perceive that providing accurate financial data will lead to a punishment: their having to pay tax.
- They are therefore motivated to withhold data (by not providing a tax return, or not providing a full tax return); or to distort data (e. g. to underestimate their income/profit or overestimate their expenditure/losses).
- Any situation in which information is felt to have a political value may also lead to it being withheld on grounds of the old adage ‘information is power’.

Perceptions of other data-related rewards

- Where performance-related pay has been instituted in the public sector, staff will rightly perceive that the provision of certain performance data (i. e. apparent performance above target) to their managers will lead to some personal reward (i. e. a pay bonus).
- In this situation they will be motivated to hide negative performance data and to inflate or make up positive performance data, thoroughly undermining the performance management system.
- Conversely, political leaders may be motivated to paint a falsely negative picture of difficulties in their district if they believe this will trigger a flow of assistance and development resources from federal or international funds.

These reward and punishment perceptions particularly affect the public sector and its clients (to whom it will often be providing money, services or other resource rewards), and compliers (whom it will often be 'punishing' via a gamut from tax bills through fines or license revocation up to imprisonment). In all these cases, the citizen's self-interest dictates that they will not be motivated to not present or handle data accurately.

All this assumes that those involved do have some perceptions, but there may be situations in which there is a lack of perception; for example, where sources do not know why data is being sought from them. They will try to work this out from situational clues, but they may guess wrong and accordingly skew the data they provide wrongly. Equally, there can be cases of lack of knowledge; for example, where sources feel motivated to provide data even though they do not have that data.

6.3.1.5 Improving Public Data Quality

what would the soft approach advocate as a way to address data quality problems in e-government systems? The key will be the perceptions and motivations of all those involved in the chain. In particular, the public agency needs to find ways to align perceptions and personal motivations with formal organizational objectives.

What mechanisms exist for doing this? Some suggestions follow, summarized in Figure 6.9.

Ensure there is a user

- Perception of data non-use is a major demotivator.

- Matters can be improved if the e-government system is redesigned to ensure that the data being gathered is actually used for decisions and actions.
- This may involve changing the content of data gathered to match the true information needs of users.

Merge stakeholder roles

- The greater the number of stakeholders in the chain, the greater the chance of motivational problems.
- Merging roles will reduce this danger.
- Those who capture the data can also be those who input the data.
- For example, where a survey was being undertaken, role merger could mean the use of handheld devices that can accept data input in the field.
- Going further, data sources can themselves capture and input data.
- Where the consumers of public services themselves become producers of their own data, the use of web-based electronic forms enables this.

Make early stakeholders into data users

- Sources, capturers and inputters typically do not use the data that depends on them.
- If they are turned into users, they have a much greater motivation to ensure the quality of system data.

Other feedback to early stakeholders

- Even if early stakeholders do not become data users, other types of feedback can motivate them.
- This can be as little as a simple word of thanks from the user, or an explanation of why and how the data is being used.

Other reward and punishment techniques

- Giving money to data sources and higher pay to data capturers, inputters and processors is one motivational technique, but money is not the only motivator.
- Punishment too can play a role, such as realistic threats of fines or imprisonment for those failing to fill or filling inaccurate tax returns, or threat of removal/reduction of budget by an audit or for failure to produce accurate audit figures.

Find alternative sources

- Identify alternative sources for the same or similar data, who/which have less self-interest in the use of the data.
- For example, get administrative staff to return data on service activities of professionals (e. g. number of clients met) rather than the professionals themselves.

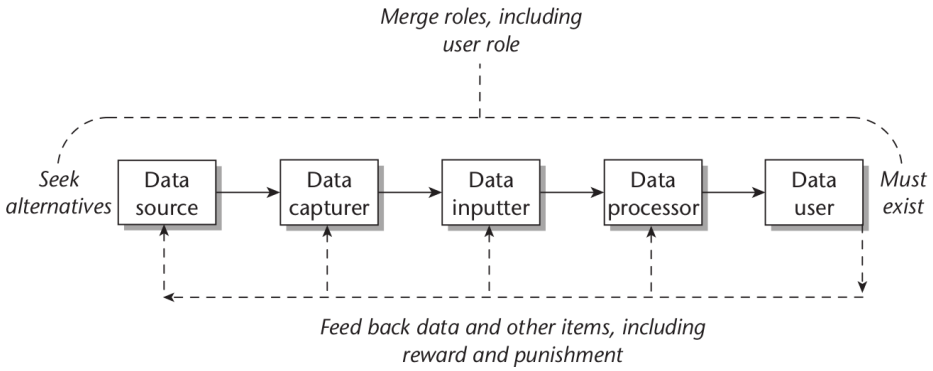


Figure 6.9: Soft approaches to improving data quality

6.4 Managing Issues for e-Government

6.4.1 Core Issues

Following are core issues that managers in the public sector have always faced:

- position (the location of the IT function within public sector organizations);

- people (recruitment and retention of staff involved with e-government);
- pelf (dealing with the financial aspects of e-government);
- projects (the ways in which e-government projects are managed);
- politics (the role of organizational power and politics in e-government).

6.4.1.1 Position

Where in the organization is the IT function to be located? There are various different possibilities.

- Decentralized location,
- Centralized location,
- Hybrid approaches to IT location.

Decentralized location At the extreme, responsibilities for e-government may be so decentralized that no organizational IT structures, staff or budgets exist: everything is left up to individual staff.

- One stage up from this is the situation in which one member of staff in each section is identified as the computer 'whizz-kid'.
- While continuing to perform their usual managerial or clerical role, they informally take on an IT1 support role.
- One stage further up, some or all of the organization's departments have their own IT staff and/or IT unit and a specific departmental IT budget.
- These resources are focused on serving the needs of the individual departments.

Centralized Location At the other extreme is the centralized IT unit.

- Such units are normally funded from a central budget.
- They are naturally larger than their decentralized counterparts.
- They may therefore be divided internally into a number of sub-units covering specialisms such as computer and network operations, systems development, data management, and strategic planning.

The location of the IT unit within the overall structure of the organization reflects attitudes to e-government in the organization, and also partly determines what the unit can and cannot achieve within the organization.

Hybrid approaches to IT location Looking within the public agency, a hybrid location can mean either a separation or integration of central and local responsibilities. For example, there could be a hybrid management structure for the IT unit, with a management group that involves internal users and senior officials as well as IT staff.

Alternatively, a hybrid structure for the IT unit could mean that it reflects the wider structure of the public agency. Thus, for example, a unit supporting a local government could have a team covering housing, another team covering public works, another covering environment, and so on.

6.4.1.2 People

People are more important than technology. eGovernment managers must therefore spend much of their time dealing with people related issues.

The planning, development and operation of any new e-government system is likely to require new competencies, thus creating a gap between the competencies staff currently hold and those they need.

Competencies can be understood in relation to three domains:

1. **Skills**: Organizations may find a skills gap in anything
    - from spotting opportunities for new e-government systems,
    - to analyzing current use of information,
    - to process redesign,
    - to software programming,
    - to system installation and use.
2. **Knowledge**: Organizations may therefore find a knowledge gap where staff do not know:
    - about systems development methods, or
    - about the nature and role of information and information systems, or
    - about organizational systems and processes, or
    - about the basics of IT, or

- about the design options that could be applied to the new e-government system, or
- about why the new system should be operated in a particular way.

3. **Attitudes**:
   - Where different stakeholders have different attitudes to the new e-government system,
   - one could talk of an 'attitude gap'.
   - In many ways this reflects the different values and objectives of different stakeholders.

Public managers face two main options in filling these competency gaps that new e-government systems create. They can:

1. Train existing staff,
2. Recruit new staff.

6.4.1.3 Pelf

Money matters loom large in e-government projects. For example, e-government has to work within the confines of public sector budgeting procedures. Related to this, e-government also has to work within the confines of available finance.

6.4.1.4 Projects

The overriding management issue for e-government projects should be the challenge of failure.

- Most e-government initiatives fail due to poor implementation and management.
- Gaps between design and reality help to explain why e-government systems succeed or fail.

6.4.1.5 Politics

e-government is far more about people and politics than it is about technology and rationality:

Sometimes, IT projects fail because of economic reasons; rarely, if ever, because of technological factors. Most usually, the failures are political in nature.

Why should there be so much politicking around e-government? In short, because two pre-conditions of politicking[2] are met.

1. First, there are interdependent groups that have different objectives and values.

2. Second, there are important but scarce resources involved.

So e-government brings together in large amounts both critical tangible resources — people, money and equipment — and critical intangible resources — information, power and kudos. They therefore form a key locus[3] for organizational politics.

6.5 Emerging Management Issues for e-Government

Followinga are the management issues that have come to prominence more in recent years.

1. **performance** (the measurement of e-government-related performance);

2. **policies** (the organizational policies that e-government managers have to develop and promote); these are divided into:

   - **policies on public data**, and
   - **policies on other issues**.

6.5.1 Performance

- Performance management is a component of public sector reform.

- It is a technique originating in the private sector that is now being promoted in the public sector.

- As with most such techniques, issues arise because some of the assumptions underlying performance management do not apply, or apply differently, in the public sector.

[2]the action or practice of engaging in political activity.
[3]a center of activity, attention, or concentration

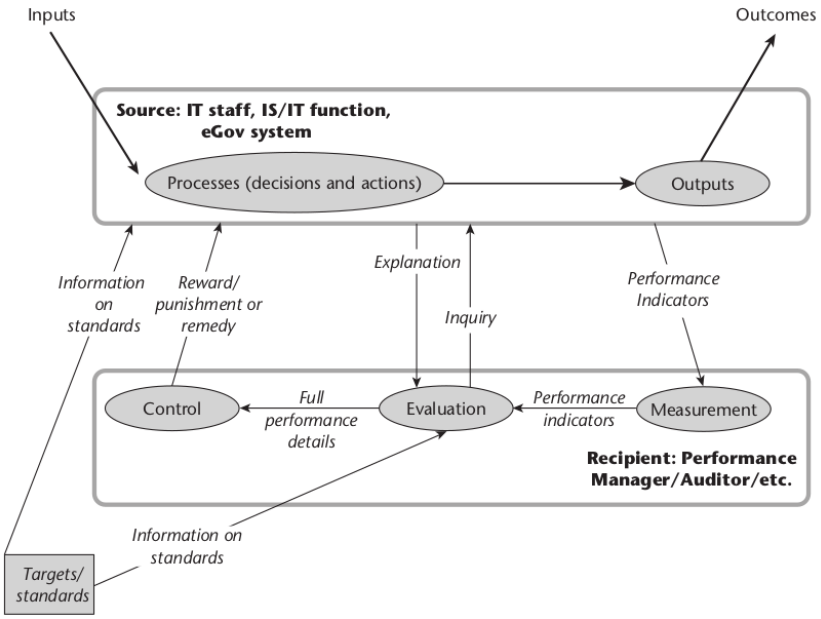


Figure 6.10: Performance management in e-government

6.5.1.1 Staff Performance

Performance management in the public sector follows a standard pattern of target setting, measurement, evaluation and control, as shown in Figure 6.10.

- In reference to IT staff management, this would involve working first on a clear job specification and then tying the major items of content (ideally those that are output related) down to measurable performance indicators and targets.
- Actual measures of performance would typically be discussed as part of regular staff-manager meetings with reasons for under and over-achievement discussed.
- Rewards would be instituted for achievement/over achievement and remedial measures for under-achievement.

6.5.2 Policies

6.5.2.1 Policies on Public Data

Public agencies operate in a sea of government laws, orders, policies and regulations. These external drivers pressurize agency e-government managers

to develop and implement their own internal policies on a wide variety of issues.

Data policies must grapple with a four way data conflict faced by public agencies, summarized in Figure 6.11.

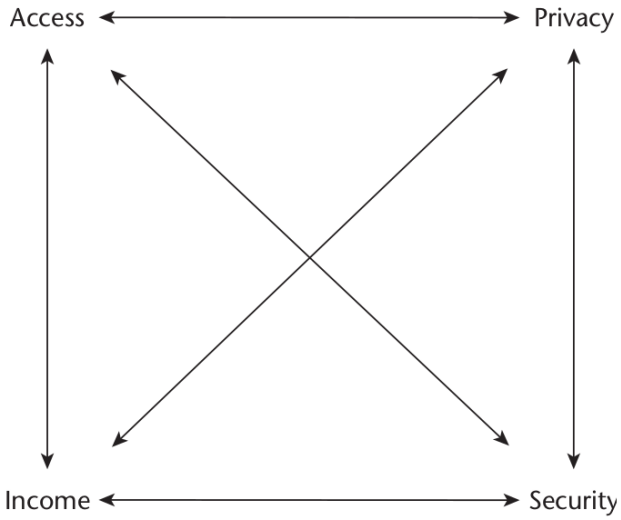


Figure 6.11: Data conflicts in the public sector

Take the income–access tension: 'Open government encourages making access easier and cheaper, while financial pressures on Departments and Agencies to recover costs and maximize returns on their information "assets" lead to controls and charging'. The more the government charges for its data, the greater the barriers to access become. Yet the wider it allows access, the less it can earn from data sales.

Following are some of the central policies that relate to access, privacy and security.

Access policies for management of data records There are two main issues that public CIOs face in creating policies for data access:

1. storage and
2. retrieval.

1. **Storage**: As regards storage, public servants have to be persuaded to treat digital data — from email messages to websites — in the same way that they treat paper: 'there has to be an audit trail, with version numbers for documents, which should be archived in read-only files so that they can't be tampered with'. Those electronic files must then be held securely and passed over to the archivists at the appropriate time.

2. **Retrieval**: The second problem arises with retrieval. Data from old storage format such as CDs, and magnetic drive will be difficult access time goes. These devices lose their data after some years and these must be copied to new system. As the pace of technological change and the use of IT in government increases, this problem will only grow.

Access policies for freedom of information In a bid to ensure access to data across the public sector (and beyond) some governments have introduced *freedom of information (FOI)* legislation.

Access policies and the digital divide IT is very much a two-edged sword as regards access to government data.

1. On the one hand it reduces barriers. IT has made it far cheaper, quicker and easier to access that data (such as downloading electronic forms from government website instead of buying paper based form).

2. On the downside, IT raises barriers and has created a digital divide across which one group reaps the benefits of IT-enabled accessibility and one group cannot.

Privacy policies for data protection Data protection legislation chimes very much with information resource management principles, and it has been a significant driver behind centralized data management. It has pressurized public agencies to identify someone senior and central who will be responsible and accountable for the accessibility, confidentiality and accuracy of data held on e-government systems.

Security policies for protection of data From Figure 6.11, we can see security may be in tension with goals of access and/or income.

The growing use of websites within e-government systems followed by the rise in global terrorism plus high-profile computer crime cases has thrown the issue right to the top of the management agenda.

6.5.2.2 Policies on Other Issues

There are many other policy issues of relevance to e-government. Here, we discuss three:

1. disability/accessibility; 2. ergonomics; and 3. Internet usage.

Disability/Accessibility New technology offers ways to overcome some of the barriers faced by people with disabilities; including barriers of access to government data and government services.

The policy requirements that relate to accessibility fall into two main types. First, there are very specific guidelines, such as those provided for e-government website design (e. g. 'avoid using images to display text', 'avoid using absolute sizes for fonts', 'specify the language of text', 'avoid using emoticons'. Second, there is a set of higher-level issues:

- **Structures**:
  - A designated agency official responsible for accessibility policies, processes and structures;
  - an external voluntary advisory committee on disability and accessibility.
- **Systems**: Processes and structures for feedback on accessibility including an email contact and a system for complaints and for dispute resolution.
- **Processes**:
  - Training of staff to raise accessibility awareness and skills;
  - ensuring procurement of compliant technology; testing of web pages and other IT before live use in e-government systems;
  - reviewing kiosks for accessibility barriers.

Ergonomics Ergonomics can be defined as using knowledge of humans' physical and psychological technology, the arrangement of the work environment, and the organization of the job. By applying ergonomics in the design of e-government systems, health problems can be reduced and efficiency can be increased.

Internet usage As public servants spend increasing amounts of their working lives online, public agencies have been pushed to develop policies guiding online activity. As with many e-government-related policies, the driver for Internet use policy often seems to come from outside public agencies. It may be partly the drive of fear of litigation; it may be partly the drive of guidance from central agencies and it may be partly mimetic effects that spread from

one agency to another. The overriding issue in all cases, though, seems to be concerns about the 'cyber-liability' of public agencies.

Liabilities may cover civil issues (such as defamation by a public servant via an email or website, or email harassment) or criminal issues (such as obscenity, spreading of computer viruses, or breach of copyright, data protection or other relevant legislation).

CHAPTER

7

IMPLEMENTING E-GOVERNMENT

7.1 e-Government System Life Cycle and Project Assessment

7.1.1 System Life Cycle

Innumerable methods for systems development have been created, with a variance here or there, but all of them correspond more or less to four core stages:

- **analysis** of what is currently happening, and of whether and why a new e-government system is needed;
- **design** of the new e-government system's components;
- **construction** of the new e-government system;
- **implementation** of the new e-government system.

Any e-government systems project seeks to create a new situation that is different from the current one. The greater the difference between the new

and current situations, the greater the degree of change that is required, and the greater the likelihood of system failure. Successfully planned e-government systems will therefore be those that require a manageable degree of change.

In order to assess this 'degree of change', the core of the systems development method consist of three activities:

1. mapping out the realities of the current situation;
2. designing a proposal for the new situation; and
3. assessing the difference between the two, and reacting to that difference.

eGovernment projects typically involve a cycle of five stages:

1. project assessment,
2. analysis of current reality,
3. design of the new system,
4. system construction,
5. implementation and beyond.

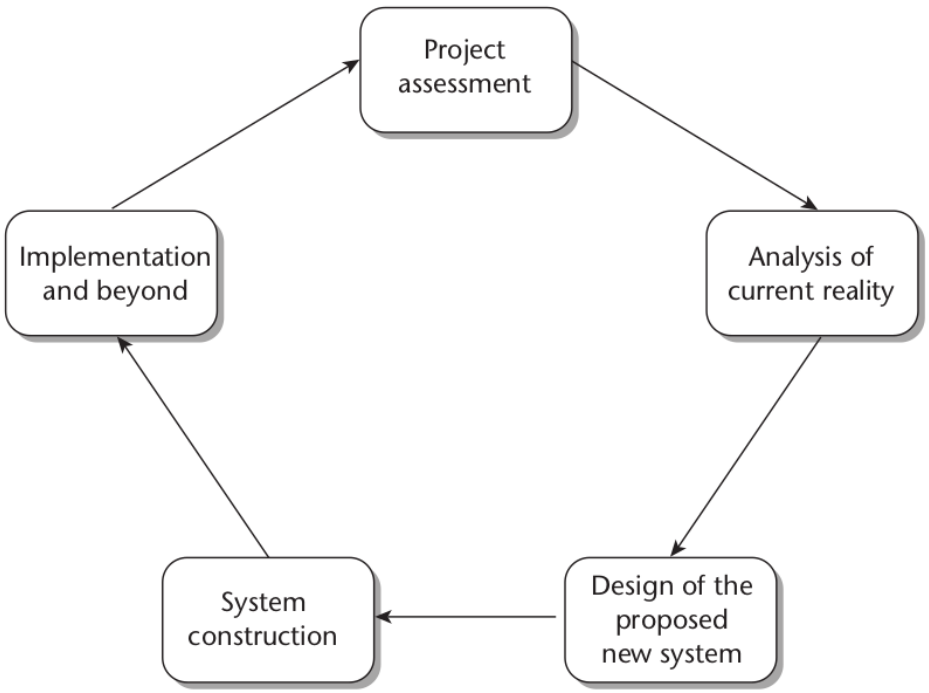


Figure 7.1: The e-government systems development lifecycle

1. **Project assessment**: Identifying possible e-government projects; outlining basic project parameters; and assessing whether or not to proceed with the project.

2. **Analysis of current reality**: Description and analysis of the seven ITPOSMO dimensions as they exist within the current situation of the organization.

3. **Design of the proposed new situation**: Setting objectives for the proposed new e-government system, and then describing in general terms how the seven ITPOSMO dimensions should be different for the new system to meet these objectives. Different options for the new system may be evaluated at this point.

4. **System construction**: Acquiring any new technology; undertaking detailed design of the new system; then building it, testing it and documenting it.

5. **Implementation and beyond**: Training users to use the new system; converting data to new formats; introducing the new system; monitoring and evaluating its performance and context; then undertaking any necessary system maintenance.

Assessing and mitigating risks (the degree of change between current reality and new proposal design) is identified as a separate activity. It could take place after general design. However, in practice, risk-related techniques are normally undertaken as an integral part of stages 1 to 3.

Overall, the stages can be called a 'systems development life cycle' because the post-implementation stages may lead to the identification of a new e-government project, thus restarting the whole process again. The life cycle is shown in Figure 7.1.

In practice, no method is as neat as this diagram might suggest because of two things.

- First, **parallelism**: activities running simultaneously. For example, analysis of current reality and general proposal design tend to overlap, with continuous analysis of the gap between the two.

- Second, **iteration**: looping back from a later step to an earlier one. For example, an issue thrown up during analysis of current reality may alter the basic project parameters and require re-assessment of the project. Alternatively, a problem during system implementation may lead to a realization that current reality needs to be re-analyzed and the e-government proposal redesigned.

No method is perfect but there are dangers for the public sector in adopting some of the harder methods. The public sector has had a tendency to choose such methods which then prove too old, inflexible, top-down, detailed, jargonized and time-consuming.

Some public sector organizations mandate that one method alone be used for systems development. In other situations, choice of method will depend on factors such as:

- **The system developer(s)**: Methods that a developer has experience of will be preferred to those that are new. Developers also have innate preferences that are relevant. Some, for instance, will prefer hard methods; others will prefer soft methods.
- **The size of system**: Small e-government systems cannot justify such a comprehensive. Instead, one or two of the most relevant aspects only need be used. The larger the system, the more one can justify a greater systems development effort.
- **The nature of the organization**: More participative, human- or user-centered methods are difficult to apply in some public sector organizational cultures. In these cases, more top-down, centralized methods are likely to be employed.

7.1.2 Project Assessment

7.1.2.1 Identifying a Project

New e-government projects typically arise in one of two ways:

- First, *identification of a problem* that needs to be solved.
- Second, *identification of an opportunity* which could be seized.

Such problems and opportunities arise from many possible sources. These sources can be any of the factors. They can arise from the external environment or from internal sources. They can be rational or political or personal. They can form part of a broader strategy or program/portfolio or stand alone.

External examples include

- complaints from citizens, politicians or the media;

- new legislation or directives or other pressures from external institutions, including those framed within the context of public sector reform;
- external economic, political or social crisis;
- technological innovation;
- observation of sister organizations; or
- the political need to project a more modern image for the organization.

Internal examples include

- a previously conducted strategic planning exercise or consultancy report;
- a survey of staff problems or suggestions;
- shortfalls in work performance measures;
- financial resources being available that need to be spent on something before financial year end;
- an individual's desire to give their career a boost; or
- an individual's desire to earn kickbacks from IT suppliers

7.1.2.2 Gathering Information on the Project

It describes the way in which information is gathered on a proposed e-government project in order to assess whether or not to proceed with it, using a basic – who, what, why — approach. If required, these can all be compiled together into an initial project proposal.

Stakeholder analysis: who is involved? Stakeholders are those individuals or groups who have a stake in the success of the new project. It is they who are the main determinant of whether the project proceeds or is scrapped, and of whether a project succeeds or fails.

A a number of possible key stakeholders are summarized in Figure 7.2. The stakeholders are:

- **Project manager/team**: Those who will analyze, design and build the e-government system.

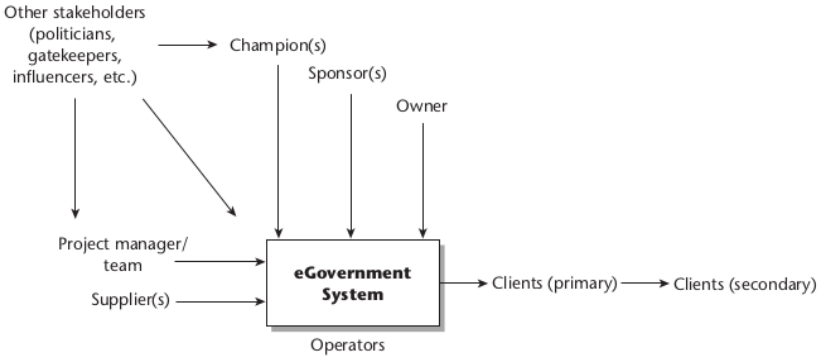


Figure 7.2: Stakeholder map for an e-government project

- **Supplier(s)**: Those who will supply the technology and other resources required by the e-government system.
- **Operators**: Those who will be carrying out the activities/processes that make the e-government system work.
- **Clients**: Primary clients are on the immediate receiving end of what the e-government system does or outputs. Sometimes these will be outside government (e. g. citizens or businesses). Sometimes, though, these will be inside government (i.e. public servants)
- **Champion(s)**: The person (or group) who drives the project on and seeks to justify its implementation.
- **Sponsor(s)**: The person (or group) who pays for the expense and effort required to develop the new e-government system.
- **Owner**: The manager of the organization or department that will own and use the system, who is ultimately responsible for the system.
- **Other stakeholders**: Who have a significant influence on the project or on whom the project will have a significant influence.

Problem statement: what is the problem? It may be useful to create a problem statement: a single sentence that tries to encapsulate who or what the problem relates to, and what exactly is wrong, without trying to define a solution. This statement may well be defined by the most powerful stakeholders.

Project Rationale: why? This is a simple definition, possibly in a single sentence, of the main objective for the new e-government system sought by the most powerful stakeholders. In most situations it would relate to alleviating the previously identified problem (or making use of the identified opportunity).

Constraint analysis: what constraints? Constraint analysis helps you understand the roadblocks that hold an e-government project back.

Constraints will vary from situation to situation. Example:

- Technology
- Staffing and skills
- Objectives and values
- Other resources

Environmental prediction: what next? A classic systems failure is to create a new e-government system suitable for today, but not for tomorrow. To guard against this, some type of 'crystal ball gazing' is required to anticipate future conditions within which the e-government application will have to operate. Typical points to be answered include:

- How long is the new system likely to last?
- How is the operation of the e-government system likely to change over its lifetime?
- What kind of changes are likely to occur within the system's environment during this timeframe?
- Given all the changes, is the e-government system likely to be sustainable?

7.1.2.3 Project Summary Statement

In thinking about and discussing a potential e-government project, it can be useful to have a single statement that summarizes the project. Such statements need to be concise enough to make them usable, but comprehensive enough to include the important aspects of the project.

7.1.2.4 Assessing the project: the 'business case'

Project Feasibility This is the first quick and dirty attempt to check the gap that exists between current reality and the new design required in order to implement the proposed e-government system. The intention is to look

at risks in order to assess whether or not it makes sense to proceed with the project.

Focusing just on some key points in the public sector, feasibility can be corralled under the PoTHOleS acronym: **P**olitics, **T**echnology, **H**ard cash (i.e. finance), **O**ther **l**esser **r**esources, and **S**ustainability. Each of these can be regarded as a pre-condition for successful development and operation of an e-government system:

- Political feasibility
- Technical feasibility
- Hard cash – financial feasibility
- Other lesser resource feasibility
- Sustainability

Project priorities One way to choose between projects is to look at their assessed feasibility, and prioritize those projects that look most feasible.

Ultimately, though, priorities may well be determined by the personal objectives of the most powerful stakeholders.

Project opportunity costs Only rarely is the question asked: 'What else could we invest these resources in if we did not invest them in this e-government project?' If the question is asked it can produce surprising results. Stakeholders may suddenly become aware that a large amount of money and time is about to be spent on something that no-one particularly wants.

Project impacts eGovernment systems are increasingly interwoven into the fabric of the public sector and, as a result, they have a growing impact on the work of the public sector. At this point in the lifecycle, then, impact assessment exercises may be conducted, such as the privacy impact assessments.

Project planning and management: how, who, what and when? Once a decision has been made to proceed further with an e-government project, plans are normally made for that project. This will typically involve decisions about:

- **How**: The approach to systems development to be used; the main stages and tasks that will have to be undertaken in order to develop any new system; and the deliverables that form their output (reports, diagrams, decisions, acquired or developed IT, etc.).

- **Who**: The staff involved in systems development from both inside and outside the organization.
- **What**: The financial, technological and other resources that will be required for development.
- **When**: The timetable that will be worked to. Project milestones can be inserted as points for project review based on time (e.g. every week), money (e.g. after a certain amount has been spent), or on the deliverables (e.g. after the project assessment, after the analysis of current reality, etc.).

7.2 Analysis of Current Reality

7.2.1 Methods of Analysis

Overview of Data-gathering Methods

There are four main data-gathering techniques that can be used to understand current reality:

1. **Interview/discussion**: Talking to individuals or groups about the current situation.
2. **Questionnair**e: Gathering background information using a survey of stakeholders.
3. **Document analysis**: Reviewing current manuals, regulations, policies, contracts, memos, reports, and so on.
4. **Observation**: Looking at what currently goes on, including the use of any current information systems.

7.2.2 Recording Techniques

The elements described above can be recorded as text. However, using diagrams offers some significant benefits, because diagrams help to simplify, formalize and communicate representations of public sector reality.

Diagrams may be used primarily for eliciting rather than recording information. First, because diagrams help clients, staff and other stakeholders to understand a situation more easily than other means. Second, because diagrams are interesting and therefore stimulate people to contribute further. Key diagram techniques are discussed below.

Reality-Specific Diagrams: Rich Pictures

A rich picture is a diagram rich in detail that represents and summarizes the most important components of a government system and its context. It is one of the few diagramming techniques that helps represent current reality, as opposed to some theoretical and rational ideal.

Design/Reality Diagrams

Can be used either to represent current reality or to summarize the new e-government system design.

It includes:

- Process map
- Data flow diagram (DFD)
- Entity-relationship diagram (ER)

7.3 Design of new e-Government system

Too many e-government systems are designed from a hard perspective — focusing design on the technology, the data it handles, and related public sector processes only. Hard approaches are attractive because they are relatively simple and easy, because they reflect the 'e' in e-government, and because they reflect the technical background of many designers. However, hard approaches often end in failure because they ignore the soft human, political factors that have such a critical impact on e-government projects.

A successful approach to e-government design must therefore be a hybrid approach: one that encompasses both hard and soft elements;

Following are five design headings:

1. objectives;
2. information;
3. technology;
4. processes; and
5. human systems (staffing, skills and management).

7.3.1 Setting Objectives

The design and development of a new e-government system requires some guiding framework. A project summary statement may provide this to some

extent, but most projects will require a set of objectives to work to. Taking account of the framework of constraints and future changes, these can be based on the previous problem statement, project rationale statement, problem analysis and/or personal objective setting.

Objectives are often stated in terms of the benefits sought from the proposed new e-government system, and may be a mirror image of any identified problems. Objectives for an e-procurement system, for example, could include:

- to reduce the time taken to procure goods and services;
- to increase the accuracy of ordering and payment; and/or
- to increase the motivation of purchasing section staff.

If there are a number of objectives, these can now be prioritized in order to provide a principal focus for subsequent system development.

7.3.1.1 Information Design

It should not be assumed that the information provided by any existing information system meets current needs. Data may be disseminated to clients because 'we have always done it that way', even if that data is of no value to either the client or the public agency. Similarly, there may be information that stakeholders would like to access, but which is not being gathered or created. Some analysis of information requirements is therefore often appropriate. The information required within the new e-government system can be planned using a set of questions about the key information functions.

Output requirements How will information outputs meet system objectives:

- Who will expect output from the new system?
- What information will they require to be output from the system?
- Why do stakeholders require this information?
- How often and when and where will the e-government system be expected to produce information output?
- In what format will the system be expected to produce information output?
- What characteristics should the information output possess?

Capture and input requirements How will input data meet output needs:

- What data will have to be input to produce the required outputs?
- Where will the data come from, and in what form, in order to produce the required outputs?
- How will data be captured and input to the e-government system?

Process requirements How will processing turn input data into output information?

Storage/Retrieval requirements How will storage hold data needed for processing and output:

- What data will be stored and retrieved in order to produce the required output?
- In what way does the data need to be stored?

Communication requirements How will data be transmitted to support other tasks:

- What data will be transmitted as part of the tasks of capture, input, processing, storage/retrieval and output?
- Where, or to whom, will the data be transmitted?
- How will it need to be transmitted?

7.3.1.2 Technology Design

This involves thinking through alternative ways in which technology can meet stated objectives and information requirements, and selecting one of the alternatives.

Software design In designing the IT component of an e-government system, software is typically the first focus because it is software that actually does the work. If hardware is designed first, there is a danger that it will not be able to run the necessary software. Three design choices must be made, as below.

1. **Type of Application**
   (a) Improved data handling
   (b) Improved decision-making
   (c) Improved interaction
2. **Method of Software Development**
   (a) Off-the-shelf package: This either works immediately on purchase or merely requires organization-specific data to be entered.
   (b) Customized package: This is an off-the-shelf package that is altered to fit organization/user needs.
   (c) Custom-built application: This is software built from scratch to meet organization/user needs.
   (d) System re-engineering: This is the redesign and rewriting of an existing software application.
3. **Operating System**

Hardware design Three main design choices need to be made, as below.

- **Computer Size**
- **Specialist Hardware**
- **Information Systems Architecture**

7.3.1.3 Process Design

This involves thinking through alternative ways in which organizational processes can meet stated objectives, and selecting one set of alternatives.

There are two groups of tasks that form key e-government processes, and about which decisions have to be made in an e-government project:

1. Core information system tasks: At least some of the tasks required will differ from those of 'current reality' because there is a move from an old to a new information system in e-government development.
2. Wider system tasks: These tasks will be placed somewhere on the untouched — optimized — redesigned — re-engineered continuum.

7.3.1.4 Human System Design

This involves thinking through alternative ways of organizing work and work structures in the new e-government system in order to meet stated objectives, and selecting one set of alternatives. Whereas the process design phase focused on what is to be done, this phase focuses on how it is to be done, and by whom.

7.3.1.5 Evaluating Proposals and Alternative Designs

Evaluation can mean identifying the extent of change required between current reality and the proposed design(s).

7.4 e-Government Risk Assessment and Mitigation

Most e-government projects fail in some way. It therefore makes sense to perform some kind of risk assessment — and mitigation where necessary — within the e-government system lifecycle.

In general terms, we can pose the following questions about risk assessment and mitigation:

- Why? The aim of risk management is to stop e-government projects failing.
- When? Assuming a typical project life-cycle of assessment–analysis–design–construction–implementation, then typically you would do a quick and dirty risk assessment during the assessment stage, and a more detailed assessment during the analysis stage.
- Who? A small team consisting of a mix of different stakeholders is the best unit to assess risk. The fewer people involved, the greater the chance that you miss an important risk. The more people involved, the higher the time and financial and other costs of the exercise.
- How? Focusing on the notion of design–reality gaps.

7.4.1 Risk Assessment Through Gap Analysis

It is not easy to analyze the gap between current reality and the design assumptions and requirements of a proposed new e-government system. There are no hard and fast rules that say ‘this gap is OK’ or ‘this gap is too large’.

Any assessment of gaps — and, hence, of project risk — must therefore be subjective, and based on opinion and experience. If one accepts this subjectivity, then rating scales can be used, as described below:

1. Using each of the seven ITPOSMO dimensions in turn, analyze two things. First, the organizational reality relating to that dimension that exists right now at the time of analysis. Second, the conceptions/requirements within the design of the e-government application.

2. For each one of the dimensions, give a numerical rating to indicate the size of the design–reality gap on that dimension. The rating for each dimension's gap can be anywhere on a scale from zero to ten.

   - 0 rating would indicate *no change* between the design proposal and current reality;
   - 5 rating would indicate *some degree of change* between the design proposal and current reality;
   - 10 rating would indicate *complete and radical* change between the design proposal and current reality.

3. The other six dimensions to be rated from 0 to 10 are:

   (a) the technology used by agency and clients;

   (b) the work processes undertaken in the agency–client system;

   (c) the objectives and values that key stakeholders need for successful implementation of the e-government application versus their current real objectives and values;

   (d) the staffing numbers and skill levels/types required by the agency and clients;

   (e) the management systems and structures required in the agency;

   (f) the time and money required to successfully implement and operate the new application compared with the time and money really available now

4. The simplest and crudest thing to do now is to add up the rating numbers for all seven ITPOSMO dimensions and interpret them according to Table 7.1.

Table 7.1: Risk ratings and outcomes for eGovernment projects

Overall rating	**Likely outcome**
57–70	The e-government project will almost certainly fail unless action is taken to close design–reality gaps.
43–56	The e-government project may well fail unless action is taken to close design–reality gaps
29–42	The e-government might fail totally, or might well be a partial failure unless action is taken to close design–reality gaps
15–28	The e-government project might be a partial failure unless action is taken to close design–reality gaps
0–14	The e-government project may well succeed

7.4.2 Risk Mitigation Through Gap Prevention or Reduction

Risk assessment through analysis of gaps is only one element. We also need to take action if there are large gaps and a high risk of failure. Options for action are summarized through **ZABC**:

- **Z**ap the project: Abandon the e-government initiative.
- **A**lter the project: Change some of the initiative parameters to try to make it more feasible.
- **B**e selfish: If the change initiative seems likely to fail but it cannot be zapped or altered, then focus on personal goals and personal gains that can be extracted from the initiative such as training, expertise and experience, money, or equipment.
- **C**hange your job: More radically if the e-government initiative seems likely to fail, change job either within the public agency to get away from the project, or to another organization

7.5 e-Government System Construction

Once a design for the proposed new e-government system has been agreed, the development cycle can proceed to the remaining stages: that of actually constructing the new system and then implementing it. The steps in system construction are:

- acquiring any necessary new technology;
- undertaking detailed system design;
- constructing the new e-government system, and
- testing and documenting the system.

7.5.1 Procurement For e-Government System

New technology now needs to be acquired if any existing IT system is not suitable and also, for software, if a new software package (rather than re-engineered system) is to form the basis of the e-government system.

The approach to acquisition needs to be decided at the start. Five options are common in the public sector.

1. **Expression of interest**: Based on an informal statement of the agency requirements.
2. **Request for proposal**: Based on a more detailed statement of requirements than the Expression of Interest.
3. **Request for tender**: With the detailed requirements and conditions to elicit a comprehensive and comparable response from suppliers.
4. **Price quotation**: A simple price request from suppliers for a specific item or items.
5. **Period contract arrangement**: This sets a time period for a relationship between public agency and supplier typically relating to the provision of particular goods and services, such as a software package or delivery of IT training.

7.5.2 Final Construction of The e-Government System

The final construction of the system involves the steps below.

- **System Installation**

  Once the technology has been acquired, it will need to be installed. For larger e-government systems, this will require considerable pre-planning and site preparation.

- **Detailed System Design**

  If the software chosen as the basis for the e-government application is an off-the-shelf package, the system development process can proceed fairly directly to implementation (though testing and documentation will be required to some extent). If not, more detailed design work is required as a precursor to system construction or customization.

  It is at this point that specific design decisions can be made relating to issues, including design of:

  - data-gathering exercises that will produce the required data for the organization;
  - general controls to protect data quality;
  - specific application controls, including validation parameters for each data element;
  - codes to be used for particular data elements;
  - other detailed operational procedures that may be required;
  - input forms and screens;
  - processing techniques required to produce information from data, with an emphasis on simplicity and flexibility;
  - output screens and other output formats;
  - other system interfaces, such as query screens; and
  - system ergonomics

    Based on all these designs, the information system for e-government can now be constructed.

- **System Testing**

  Most system testing focuses on testing whether the output produced by the system is correct, either in terms of the information it produces or the transactions it supports.

- **System Documentation**

  There are three main types of system documentation on which work can be started right from the early stages of the development life cycle.

  - Overall Project Documentation: This is a collection of all the project documents used in developing the new e-government system.
  - System Design Documentation: This records technical information about the design and workings of the new e-government system.
  - System Operation Documentation: This records details about how to use the e-government system.

7.5.3 Introduction of The e-Government System

It involves:

- Operational Training: Training for e-government can be planned by answering a series of questions.
  - Who is to be Trained?
  - Why are they being Trained?
  - Who will Deliver the Training?
  - When and Where will Training be Delivered?
  - What will be the Specific Content of Training Sessions?
- Handover Method: There are five different methods for switching over from old to new:
  - Parallel Running
  - Phased Volume Approach
  - Phased Functional Approach
  - Pilot Approach
  - 'Big Bang'
- Data Conversion: This involves converting old system data so that it can be used by the new system.

7.6 Implementation and Beyond

7.6.1 Marketing and Support

Marketing of e-government can use much the same guidelines as other forms of marketing:

- Publicizing simple messages for mass awareness raising through all forms of advertising from print to radio/TV to email/web.
- Carrying out targeted marketing through direct mail, direct e-mail or call center marketing to specific client groups.
- Using word-of-mouth by getting staff when dealing with clients or with colleagues, or managers when giving presentations, to keep selling the system.
- Selling benefits not features, for example not 'we've got a portal' but 'now you don't have to queue'.
- Providing incentives.

Marketing alone, though, is not enough. In addition, there must be continuous provision of user support. This can take the form of a user support/information center. More typically, it is a staffed help desk and help line plus supporting documentation.

Increasingly, support is going online — documentation can be provided online, supplemented by frequently asked questions (FAQs).

7.6.2 Upgrades

One of the problems that public agencies face over time with e-government systems is that many items of IT are subject to rapid technical change, particularly software packages. The producers of such packages feel the need, because of competitive pressures, to bring out continuous upgrades to these packages. Such upgrades may be minor amendments every few months or major new versions every year or so.

7.6.3 Monitoring, Evaluation and Maintenance

Once a new e-government system has been implemented, an immediate evaluation can be carried out to see

- whether it is operating, and
- whether it is operating as intended.

System Maintenance

Any fairly minor changes that have to be made to the e-government system after its introduction are regarded as *system maintenance*. They may be:

- **Debugging**: A response to ways in which the system does not perform as originally intended; this typically involves removing programming code errors that have been accidentally included.
- **Tweaking**: Improving system performance to make it operate more efficiently.
- **Updating**: Altering the system because of changes in its original parameters

Maintenance can also include:

- **Correcting**: Making the system run as it was intended to, but does not, due to poor system development.

7.7 Developing e-Government Hybrids

The hybrid approach to managing e-government is a successful third way between two less successful extremes, covering six **POSSET** aspects: philosophy, organizational level, stakeholders, sector, extent of change, and technology.

A hybrid approach must unite the 'e' and the 'government' of e-government, avoiding failures that arise through divisions between IT staff and mainstream public officials.

- **Philosophy**: eGovernment hybrids steer a middle way between the 'hard' ideas of objectivity and rationalism, and the 'soft' ideas of subjectivity and personalized politics.
- **Organizational leve**l: eGovernment hybrids steer a middle way between top-level centralized approaches, and bottom-up decentralized approaches.

- **Stakeholders**: eGovernment hybrids steer a middle way between the interests of external stakeholders (such as clients, taxpayers, voters), and internal stakeholders (such as staff and senior officials).
- **Sector**: eGovernment hybrids steer a middle way between respecting the particular goals and values of the public sector, and accepting that some lessons and ideas can be adapted from the private sector.
- **Extent of change**: eGovernment hybrids steer a middle way between the apathy of sticking with the current status quo/reality, and the risks of failure that can be associated with new system designs.
- **Technology**: eGovernment hybrids steer a middle way between idolizing technology so much that it is the central focus of public sector change, and ignoring the technology so much that it is unable to make a contribution to change.

Despite its shortcomings, the notion of the e-government hybrid is valuable. A more hybrid approach to management will reduce the risks of e-government failure.

CHAPTER

8

DATA WAREHOUSING AND DATA MINING IN GOVERNMENT

8.1 Introduction

Data warehousing and data mining are the important means of preparing the government to face the challenges of the present world.

Data warehousing and data mining technologies have extensive potential applications in the government-in various Central Government sectors such as Agriculture, Rural Development, Health and Energy and also in State Government activities. These technologies can and should therefore be implemented.

Data Warehousing

Data warehousing is a collection of *decision support* technologies, aimed at enabling the *knowledge worker* (executive, manager, analyst) to make better and faster decisions. Data mining potential can be enhanced if the appropriate data has been collected and stored in a data warehouse. A data warehouse is a relational database management system (RDBMS) designed specifically to meet the needs of transaction processing systems. It can be loosely de-

fined as any centralized data repository which can be queried for business benefit. Data warehousing is a new powerful technique making it possible to extract archived operational data and overcome inconsistencies between different legacy data formats. As well as integrating data throughout an enterprise, regardless of location, format, or communication requirements it is possible to incorporate additional or expert information.

In addition to a relational database, a data warehouse environment includes an extraction, transportation, transformation, and loading (ETL) solution, an online analytical processing (OLAP) engine, client analysis tools, and other applications that manage the process of gathering data and delivering it to business users.

ETL Tools are meant to extract, transform and load the data into Data Warehouse for decision making. Before the evolution of ETL Tools, the above mentioned ETL process was done manually by using SQL code created by programmers. This task was tedious in many cases since it involved many resources, complex coding and more work hours. On top of it, maintaining the code placed a great challenge among the programmers.

These difficulties are eliminated by ETL Tools since they are very powerful and they offer many advantages in all stages of ETL process starting from extraction, data cleansing, data profiling, transformation, debugging and loading into data warehouse when compared to the old method.

A common way of introducing data warehousing is to refer to the characteristics of a data warehouse as set forth by William Inmon, author of Building the Data Warehouse and the guru who is widely considered to be the originator of the data warehousing concept, is as follows:

- Subject Oriented
- Integrated
- Nonvolatile
- Time Variant

Data warehouses are designed to help you analyze data. For example, to learn more about your company's sales data, you can build a warehouse that concentrates on sales. Using this warehouse, you can answer questions like "Who was our best customer for this item last year?" This ability to define a data warehouse by subject matter, sales in this case, makes the data warehouse *subject oriented*.

Integration is closely related to subject orientation. Data warehouses must put data from disparate sources into a consistent format. They must resolve such problems as naming conflicts and inconsistencies among units of measure. When they achieve this, they are said to be *integrated*.

For instance, in one application, gender might be coded as "m" and "f" in another by 0 and 1. When data are moved from the operational environment

into the data warehouse, they assume a consistent coding convention e.g. gender data is transformed to "m" and "f".

Nonvolatile means that, once entered into the warehouse, data should not change. This is logical because the purpose of a warehouse is to enable you to analyze what has occurred.

In order to discover trends in business, analysts need large amounts of data. This is very much in contrast to online transaction processing (OLTP) systems, where performance requirements demand that historical data be moved to an archive. A data warehouse's focus on change over time is what is meant by the term *time variant*. The data warehouse contains a place for storing data that are 10 to 20 years old, or older, to be used for comparisons, trends, and forecasting. These data are not updated.

Data Mining

The term data mining has been stretched beyond its limits to apply to any form of data analysis.

Extraction of interesting information or patterns from data in large databases is known as data mining. Data mining is concerned with the analysis of data and the use of software techniques for finding patterns and regularities in sets of data. It is the computer which is responsible for finding the patterns by identifying the underlying rules and features in the data. The idea is that it is possible to strike gold in unexpected places as the data mining software extracts patterns not previously discernable or so obvious that no-one has noticed them before.

Data mining analysis tends to work from the data up and the best techniques are those developed with an orientation towards large volumes of data, making use of as much of the collected data as possible to arrive at reliable conclusions and decisions. The analysis process starts with a set of data, uses a methodology to develop an optimal representation of the structure of the data during which time knowledge is acquired. Once knowledge has been acquired this can be extended to larger sets of data working on the assumption that the larger data set has a structure similar to the sample data. Again this is analogous to a mining operation where large amounts of low-grade materials are sifted through in order to find something of value.

Applications of Data Mining

Data mining has many and varied fields of application some of which are listed below.

Sales/Marketing

- Identify buying patterns from customers
- Find associations among customer demographic characteristics
- Predict response to mailing campaigns
- Market basket analysis

Banking

- Credit card fraudulent detection
- Identify 'loyal' customers
- Predict customers likely to change their credit card affiliation
- Determine credit card spending by customer groups
- Find hidden correlation's between different financial indicators
- Identify stock trading rules from historical market data

Insurance and Health Care

- Claims analysis i.e., which medical procedures are claimed together
- Predict which customers will buy new policies
- Identify behavior patterns of risky customers
- Identify fraudulent behavior

Transportation

- Determine the distribution schedules among outlets
- Analyze loading patterns

Medicine

- Characterize patient behavior to predict office visits
- Identify successful medical therapies for different illnesses

8.2 National Data Warehouses: Census Data, Prices of Essential Commodities

A large number of national data warehouses can be identified from the existing data resources within the Central Bureau of Statistics.

Census Data

The Central Bureau of Statistics compiles information of all individuals, villages, population groups, etc. This information is wide-ranging such as the individual-slip, a compilation of information of individual households. A data warehouse can be built from this database upon which OLAP techniques can be applied. Data mining also can be performed for analysis and knowledge discovery.

As the census compilation is performed once in ten years, the data is quasi-static and, therefore, no refreshing of the warehouse needs to be done on a periodic basis. Only the new data needs to be either appended to the data warehouse or alternatively a new data warehouse can be built.

There exist many other subject areas within the census purview which may be amenable and appropriate for data warehouse development, OLAP and data mining applications on which work can be taken up in the future.

Central Bureau of Statistics (CBS)

National Statistical System (NSS) is the ensemble of statistical organizations and units within a country that collect, process and disseminate official statistics on behalf of national government. An effective and efficient national statistical system that provides regular and reliable data is an important indicator of good policies and a crucial component of good governance. Central Bureau of Statistics (CBS) is the nodal agency of Nepal to collect, compile and disseminate socio-economic data in Nepal. It is involved in conducting surveys and censuses since last six decades. A number of other Ministries and Government Agencies are also involved in producing statistics relevant to their field. Some of the collected statistics by CBS under NSS are:

- Census data
- Health statistics
- Educational statistics
- Poverty measurement statistics
- Civil registration and vital (birth, death, marriage, migration and divorce) statistics
- Crime statistics

- Tourism information statistics
- Agriculture and rural development statistics
- Trade statistics
- Industrial statistics etc.

Prices of Essential Commodities

The Ministry of Agriculture, Government of Nepal, compiles daily data. Essential commodities means all the basic things that are used in our day-to-day life like food items rice, pulse, oil, spices, vegetables, fruits etc and other costs like transportation cost, health and medicine cost, education cost etc. Government collects prices of those essentials from all over the country by their agent and forecast the average cost of those essential commodities. They also analyze those prices with last year data to know by how much the price is increased/decreased this year and may forecast what may be the price increase/decrease in next year. So it helps the plan and policymaker to improve the economic growth rate.

8.3 Other Areas for Data Warehousing and Data Mining

8.3.1 Agriculture

The Agricultural Census performed by the Department Of Agriculture, Government of Nepal, compiles a large number of agricultural parameters at the national level. District-wise agricultural production, area and yield of crops is compiled; this can be built into a data warehouse for analysis, mining and forecasting. Statistics on consumption of fertilizers also can be turned into a data mart.

Data on agricultural inputs such as seeds and fertilizers can also be effectively analyzed in a data warehouse. Data from livestock census can be turned into a data warehouse. Land-use pattern statistics can also be analyzed in a warehousing environment. Other data such as watershed details and also agricultural credit data can be effectively used for analysis by applying the technologies of OLAP and data mining.

Thus there is substantial scope for application of data warehousing and data mining techniques in Agricultural sector.

8.3.2 Rural Development

Data on individuals below poverty line (BPL survey) can be built into a data warehouse. Drinking water census data (from Drinking Water Mission) can be effectively utilized by OLAP and data mining technologies. Monitoring and analysis of progress made on implementation of rural development programmes can also be made using OLAP and data mining techniques.

8.3.3 Health

Community needs assessment data, immunization data, data from national programmes on controlling blindness, leprosy, malaria can all be used for data warehousing implementation, OLAP and data mining applications.

8.3.4 Planning

At the Planning Commission, data warehouses can be built for state plan data on all sectors: labour, energy, education, trade and industry, five-year plan, etc.

8.3.5 Education

In education sector, data warehouse can be built to store large volume of historical data, analyze historical events, language research, educational status of the country, etc.

8.3.6 Commerce and Trade

Data bank on trade (imports and exports) can be analyzed and converted into a data warehouse. World price monitoring system can be made to perform better by using data warehousing and data mining technologies. Provisional estimates of import and export also be made more accurate using forecasting techniques.

8.3.7 Other Sectors

In addition to the above mentioned important applications, there exist a number of other potential application areas for data warehousing and data mining, as follows:

Tourism

Tourist arrival behaviour and preferences; tourism products data; foreign exchange earnings data; and Hotels, Travel and Transportation data.

Programme Implementation

Central projects data (for monitoring).

Revenue

Customs data, central excise data, and commercial taxes data (state government).

Economic affairs

Budget and expenditure data; and annual economic survey.

Audit and accounts

All government departments or organizations are deeply involved in generating and processing a large amount of data. Conventionally, the government departments have largely been satisfied with developing single management information systems (MIS), or in limited cases, a few databases which were used online for limited reporting purposes. Much of the analysis work was done manually by the Department of Statistics in the Central Government or in any State Government. The techniques used for analysis were conventional statistical techniques on largely batch-mode processing. Prior to the advent of data warehousing and data mining technologies nobody was aware of any better techniques for this activity. In fact, data warehousing and data mining technologies could lead to the most significant advancements in the government functioning, if properly applied and used in the government activities. With their advent and prominence, there is a paradigm shift which may finally result in improved governance and better planning by better utilization of data. Instead of the officials wasting their time in processing data, they can rely on data warehousing and data mining technologies for their day to-day decision-making and concentrate more on the practical implementation of the decisions so taken for better performance of developmental activities. Further, even though various departments in the government (State or Central) are functionally interlinked, the data is presently generated. Maintained and used independently in each department. This leads to poor (independent) decision-making and isolated planning. Here in lies the importance of data

warehousing technology. Different data marts for separate departments, if built, can be integrated into one data warehouse for the government. This is true for State Government and Central Government. Thus, data warehouses can be built at Central level, State level and also at District level.

CHAPTER

9

CASE STUDIES AND APPLICATIONS OF E-GOVERNMENT SYSTEM

9.1 Nepal

9.1.1 Cyber Laws

Cyberlaw is the generic name given to the laws governing the acts that happen and exist in the intangible digital world. The cyberlaws govern aspects such as giving a legal status to the intangible information that exist in the cyberspace, the security and privacy of such information, the relationships and contracts between persons who exchange such information, their rights and responsibilities, crimes relating to damages caused to cyber information and digital assets and all such matters related to the digital world. Cyberlaws are significant and valid not only for regulating cyber matters within countries and states, but are equally essential for resolving issues that arise in cross-national transactions. The need for cyberlaws arises from the singular fact that the laws made for the corporeal world do not take care of several of the actions that happen in the cyberspace.

9.1.1.1 Need For Cyberlaw

- Protection of Public Order and Decency
- Protection of Privacy of Individuals
- Providing Legal Status to Digital Identities and Transactions

9.1.2 ICT Development Project

Asian Development Bank(ADB) and the Government of Nepal(GoN) entered a Grant agreement on May 23^{rd} 2008 with amount of US $\$\ 2,50,00,000$ (२ करोड ५० लाख डलर) for the ICT Development project. GoN matched the grant by adding an amount of $\$\ 62,00,000$ for the project. The outcome of the project was to:

- Make ICT more accessible, affordable, inclusive, sustainable, and useful to remote and rural communities.
- Make public services more citizen-centric and business-friendly through ICT.
- Improve accessibility, efficiency, and transparency in Government service delivery with the application of ICT.
- Enhance ICT business and industry.

The Project comprised of the following Parts:

PART 1 : **Rural e-Community**

- Wireless Broadband Network
- Village Networks
- Tele-centers
- Community Mobilization and Capacity Development

PART 2 : **Government Network**

- Government Information and Data Center
- Government Groupware

PART 3 : **e-Government Applications**

- Government Enterprise Architecture

- National Identification System
- Public Service Recruitment Management System
- Land Records Management System
- Online Vehicle Registration and Driving Licenses

PART 4 : **Human Resource Development for e-Governance**

- Build awareness, knowledge and skill of stakeholders
- Establish computer labs for capacity development of training institutions
- Revise existing training curriculum of training institutions etc.

The project has been revised on 28 February, 2013. The Rural e-Community part of the project from the scope of ADB's ICT Development Project has been excluded from the project plan mainly due to duplication of effort from other Government and private sector.

Some G2C Projects of e-Government

- NID Implementation
- E-Registration System
- Online Passport Application System
- Social Insurance Information System
- e-Vehicle Registration
- e-Driving License Examination
- e-Pension etc

Some G2B Projects of e-Government

- Central e-Procurement system
- e-Customs
- Online Business Registration, renewal and approval management system
- Public service recruitment, training and employment information system

Some G2G Projects of e-Government

- Formulate directive and perform IT Audit of government IT Systems
- Test existing and upcoming government software to ensure that they meet
- e-Tax
- Immigration Management System
- e-Land
- e-MIS, Groupware, e-Pollution, e-Authentication, KMS and GIS

1. **National Portal**: It is a government website that will act as the single window (one-stop-shop) for all government e-Services and electronic information of Nepal to be delivered to citizens (G2C), business (G2B) and government employees (G2E). Delivery of e-Services will enable increased citizen participation and attempt to create an open, transparent environment through integration of different government information systems and services.

2. **Inland Revenue Department (e-VAT, e-PAN, e-Filling, e-TDS)**: The IRD is responsible for the administration of Value Added Tax, Income Tax, and Excise Duty. All these taxes can now be entered online through the web application developed by IRD. This has made taxpayers job easier.

3. **Department of Foreign Employment**: All the information of Department of Foreign Employment is made public and put in the website. It has an online application to track the record of an foreign employee through their passport number and permit number.

4. **Machine Readable Passport**: Department of Passport has been issuing Machine Readable Passports (MRPs) as per the guidelines of ICAO Machine Readable Travel Document. To effectively carry on this job, the Ministry of Foreign Affairs has awarded the contract to 'Oberthur Technologies' of France, a globally renowned company in the field of smart card technology and associated services, which personalizes the Nepalese Machine Readable Passports to the Department of Passport.

5. **Government Accounting System (FCGO)**: Financial Comptroller General Office (FCGO) is the main agency responsible for the Public Financial Management (PFM) system of Government of Nepal (GoN). IT based Government Accounting System (CGAS) has also been designed and is executed. This captures transactions and their accounting, book keeping, reporting in respect of expenditure, revenue, and retention money in these units.

6. **e-Procurement**: PPMO has developed an online portal for all the works related to public procurement. It has a portal https://bolpatra.gov.np which gives a web interface for all services. E-procurement web portal of is designed to facilitate the bidder to submit their bids through e-submission.

7. **Public Service Commission**: Many processes of Public Service Commission are now going online. It includes online application, result viewing etc.

8. **National ID**: National ID project is aimed at providing a single identification smart card to all the citizens which will contain all information regarding the citizen.

9. **e-Passport**: e-Passport is aimed at digitizing the current passport system. All the information regarding citizen's passport will be available digitally via online application.

9.1.3 Government Integrated Data Center (GIDC)

It's a National Data Center for Nepal for the first time in the whole history of ours, built with the help of the KOICA, Korean Government. The name given for this Data Center is Government Integrated Data Center (GIDC). This project was started on 14^{th} May, 2008.

It has mainly three types of Data Centers:

- **Internet Data Center (IDC)**: It provides data and Internet services for other companies

- **Storage Data Network (SDN)**: It is network of interconnected storage devices and data servers usually located within an enterprise data center or as an off-site facility offering leased storage space.

- **Enterprise Data Center (EDC)**: This is the central processing facility for an enterprise's computer network.

Objectives

The objectives of GIDC are:

- Minimize investment cost by using GIDC based common facilities
- Improve stability and efficiency through concentrated central management within Data Center that provide Internet access and management for e-government
- Minimize operation cost by means of centralized GIDC
- Offer easy expansion and upgrade for increasing demands
- Offer basic environment for government co-location and integrated government mailing service

Features

Features of GIDC:

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

Facilities

Facilities of GIDC:

1. **Information Technology System**:
    - Routers, Backbone Switches etc.

- Integrated Network Management System
- Integrated Server Management System
- Integrated Storage
- Integrated Back-up
- High level firewall with security for different attacks and threats

2. **Infrastructure System**:
   - Air-Circulation System : HVAC (Heating, Ventilating, and Air Conditioning)
   - Security: Biometric Access Control System, Card Reader Access Control System, CCTV
   - Main Monitoring Room: Integrated Console
   - Facility Management System: Water Leakage Sensing
   - Disaster Prevention System: Fire-Fighting
3. **Electrical System**:
   - Auto Load Transfer Switch
   - Main Power Switchboard (3 Transformers)
   - Emergency Generator: $400KW$
   - UPS: $200KVA$
   - Batteries: $480nos.$

Security

To guard against line failure or intrusion, the data center is staffed 24 hours a day. Movement throughout the facility is escorted at ALL times. There is 24×7 closed circuit monitoring of all areas and entrances. Between the cameras, access control, and the security team, the data center facilities are pretty secure. Along with the physical security there is multi layered logical security system to prevent any data loss. There are high level firewall devices to limit access to different services and logging devices to keep track of everything that is happening inside the system.

The Figure 9.1 shows the different levels of logical security for the protection of data inside NITC. There are seven layers of Security Services provided by NITC including firewall and anti-spam security. These layers provide complete content protection along with integrated management, logging & reporting.

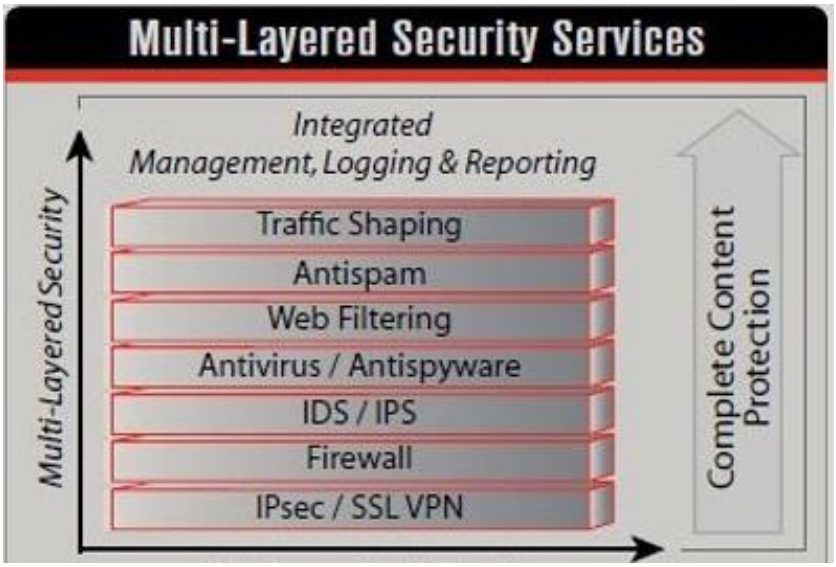


Figure 9.1: GIDC security features

9.1.4 e-Government Master Plan

The e-Governance Master Plan for the Government of Nepal was previously formulated by Korea IT Industry Promotion Agency (KIPA) working with the then High Level Committee for Information Technology (HLCIT) for the years 2007 - 2011. KIPA had signed a MOU with the then High Level Commission for Information Technology (HLCIT) for the said task.

eGMP2

After a rigorous review and analysis of the e-Government Master Plan 2007 – 2011 and analysis of the prevailing policies, acts and regulations concerning ICT and e-Governance, the team determined areas that required intervention and update and projects that need to be implemented for e - Governance to be successfully realized in Nepal.

Four pillars of eGMP2

Sustainability

- Demand Responsive / Self-ownership Projects (Bottom Up Approach)
- Shared Benefits (Citizen / Business, Government / Employees, Social / Economic)

- Services outsourced / Local Technical Availability
- Assurance of AMC

Capacity building

- Awareness Campaigns (Citizen/Business)
- Chief Information Officers (CIO) in every Government of Nepal (GON) Centers & IT Cell
- HRD and Motivation

Service delivery

- Client satisfaction surveys
- Rewards for accomplishes
- Use of new technology and media for better deliver

Implementation

- Top Management Commitment
- Motivation for efficiency in work
- Monitoring and Evaluation (M&E)

9.1.5 Human Resource Management Software

यो शीर्षक अस्पष्ट भएकाले कुनै सामग्री फेला पार्न सकिएन।

9.2 India

9.2.1 Community Information Centers

A project of connecting the blocks of the District through ICT was launched in 2000 and accordingly a Community Information Centre (CIC) were also

setup in Dibang Valley District. Under Phase-1 project, Mipi-Anini-Aliney Block was selected setup. Under various natural stress and strain, the project was completed in 2002 and have been operational since then. The main feature of the CIC has been the internet and email services provided in such mountainous and terrain geography where telephone service is a far off dream for a common man. The rural youths can now get connected to the rest of the world with a click of button and get any information needed. For example, when the CBSE results were declared, the students got their results sitting in their schools or Block Hqr within no time. Prior to setting up of CIC, they had to face the hardship of making long journeys to Roing, in Lower Dibang Valley District and then stand on long queues to know their results, or they had to wait for more than a month for the results to arrive at their school. Another benefit has been confirming train reservation status[1].

Objectives

The project aims to achieve the following objectives:

- ICT Infrastructure at Block level
- Web Access and Internet Services such as E-mail
- Market Access and E-commerce
- Access to Socio-Economic Databases
- E-learning (Computer Aided Learning Processes) and E-education
- E-medicine, E-consulting
- E-governance applications, Government to Citizen (Citizen Centric) services
- Weather Information
- IT awareness among local people
- Computer Training Programmes
- Tender Notification
- E-employment Notification

Infrastructure and Management

The Centre is well-equipped with infrastructure including one server machine, five client systems, one each of a VSAT, Laser Printer, Dot Matrix Printer, modem, LAN hub, TV, Webcam and two UPS (1KVA, 2 KVA). The CIC is looked after by CIC Operators (CICOs) for managing the centres and providing services to the public.

[1]https://dibangvalley.nic.in/egov-initiatives/cic/

The project is a joint effort by Department of Information Technology (DIT) under Ministry of Communications and Information Technology (MCIT, now Ministry of Electronics & Information Technology-MEITY), National Informatics Centre (NIC) and the State Governments of the North-Eastern states.

DIT funded the project and had the responsibility of overall monitoring and management. NIC was the Implementation agency. Application Software development and Training of CIC Operators were a part of NIC's responsibilities. The State Governments were entrusted with the mandate of site selection, preparation and maintenance, manpower recruitment and identification and creation of content for various services/applications to be delivered through the CIC.

Future Plans

It is proposed to use the Community Information Centres for e-Entertainment in the future. A select bouquet of channels could be telecast through the VSAT based network as TVs with other associated infrastructure is already available at the CIC. Other future prospects are the provision of connectivity to Schools and Block Offices.

9.2.2 e-Procurement in The Government of Andhra Pradesh

The state of Andhra Pradesh identified e-procurement as a core e-government project with a view to introducing transparency and accountability in its procurement operations which amount to about $2 billion (२ अरब डलर) annually. It is decided to adopt a Public-Private Partnership (PPP) model for implementation of the concept. After evaluating the proposals of the 12 e-procurement players in the world, it selected the affiliate of Commerce One in India — C1 India Ltd. — to implement the project.

C1 India, set up the required infrastructure and hosted the e-procurement marketplace. Initially, four major procuring agencies, dealing with public works, medicines, computers and transportation were selected for the pilot. The scope of the pilot includes registration of suppliers, market making, training of the suppliers and employees of the buying agencies and introduction of end-to-end procurement capabilities in the portal. The current features include online notification of all tenders, online filing of tenders, auctions and reverse auctions. The partner gets compensated at a fixed percentage of the value of goods and services procured.

The e-Procurement project of Andhra Pradesh, went on to expand its purview to serve over 90% of the procurement Government. It evolved into a sophisticated system with enhanced security features, analytical capabilities and a digital signature requirement that is mandatory for all users-buyers and suppliers as well. The project continues to be vibrant and is serving the increasing online procurement needs of the Government.

9.2.3 e-Suvidha

E-Suvidha Project has been envisaged with the main aim of benefiting urban citizens at each district of the state and to offer various governmental services both at city as well as district level within the state. Its main objectives are as follows:

- To provide 'Single window all utilities' system at all the counters of the systematic and well integrated Citizen Service Centres (E-Suvidha Centre) installed at prime locations within the state adjacent to public houses and workplaces that offers computerized information regarding various government departments, semi-government departments, institutional departments, authorized organizations, self-financing departments, integrated information related to selected corporations and bodies, allows settlement of bills, Government payments (G2C) and professional services of private entities (B2C) through the use of information technology.

- To benefit the urban citizens with the above stated services in all the districts of the state and to offer various governmental services both at city and district level.

This project has been established as the subordinate official society of Information Technology (IT) and Electronics Department, Government of Uttar Pradesh under Societies Registration Act 1860, and is popularly known as E-Suvidha.

Under E-Suvidha Project citizens are offered various bill payment services of different departments all at one place i. e. at e-suvidha centre where 'Single Window all Utilities' system is followed whereby citizens don't have to visit different departments for submitting the bills. Presently, this facility is operated through setting up of intranet but in near future it has been proposed that all the services would be made available to the citizens on their residences only via internet.

Vision

The vision of e-Suvidha project is "to provide to the citizens of Uttar Pradesh, all G2C and G2B One-Stop services and information of Departments and agencies of Central, State and Local Governments in an efficient, reliable, transparent and integrated manner on a sustained basis, with certainty, through easy access to a chain of computerized Integrated Citizen Service Centers (ICSC's) and through multiple delivery channels like Electronic Kiosks, mobile phones and the Internet". The vision of e-Suvidha is to eventually bring all the G2C, G2B and B2C services within the purview of the project as a single interface to obviate the need for citizens and business people to visit the Government offices except for specialized and complex services

e-Suvidha Services

G2C Services

- Revenue Department
- Urban Development Department
- Medical & Health Department
- Social Welfare Department
- Women Welfare & Child Development Department
- Handicap Welfare Department
- Employment Department
- Food & Civil Supplies Department
- Panchayati Raj Department
- Labour Board
- All Concerned departments with respect to e-District

B2C Services

- PAN Card
- Aadhar Card
- LIC Premium Collection
- Mobile Top-up/Recharge
- Internet Data Card Recharge
- Mobile bills payment

9.3 Other Countries

परीक्षा नजिकिएकाले यी शीर्षक भित्रका कुनै पनि सामग्री खोजतलास गरिएन।

9.3.1 E-Government Development in South Korea

Assignment

9.3.2 e-Government in China

Assignment

9.3.3 e-Government in Brazil

Assignment

9.3.4 e-Government in Sri Lanka

Assignment

9.3.5 e-Government in Singapore

Assignment

9.3.6 e-Government in USA

Assignment

PURBANCHAL UNIVERSITY

2018/ २०७५

4 Years Bachelor of Computer Application (BCA/Eighth Semester/Final)

Time: 3.00 hrs. Full Marks: 80 / Pass Marks: 32

BCA451CO, e-Governance

Candidates are required to give their own answers in their own words as far as practicable. Figure in the margin indicate full marks.

Group A

Answer TWO questions. **$2 \times 12 = 24$**

1. Compare between e-Government with e-Commerce. Explain development stages of e-government and barriers of e- Government implementation with example.

2. Explain network infrastructure. Why e-Government architecture and interoperability frameworks are needed for e-Government infrastructure development? Explain with an example.

3. Discuss e-government security architecture. Also explain the challenges to implement e-government system.

Group B

Answer SEVEN questions. **$7 \times 8 = 56$**

4. Describe importance of e-Readiness with e-Readiness framework. Explain issues in e-government readiness.

5. What is PPP? Describe citizen-centric approach to e-Government adoption.

6. Explain management approaches of e-Government system. Describe emerging management issues for e-Government system.

7. Explain the e-Government risk assessment and mitigation with an example.

8. What are the major task involved in implementing e-Government. Describe analysis of current reality.

9. Show comparative analysis of e-Government development in South Korea and China.

10. What is e-Government system life cycle? Explain security management model in detail.

11. Write short notes on any TWO:

    (a) e-Government master plan

    (b) Managing public data in e-Government.

    (c) Impact of e-Suvida and Cyber Laws in Nepal

PURBANCHAL UNIVERSITY

2019/ २०७६

4 Years Bachelor of Computer Application (BCA/Eighth Semester/Final)

Time: 3.00 hrs. Full Marks: 80 / Pass Marks: 32

BCA451CO, e-Governance

Candidates are required to give their own answers in their own words as far as practicable. Figure in the margin indicate full marks.

Group A

Answer TWO questions. **$2 \times 12 = 24$**

1. Differentiate e-Governance and e-Government. How e- government helps to improve economic condition of Nepal? Explain Development stages of c-Government.

2. What is importance of data centers? Explain e-Government architecture and interoperability frameworks with an example in e-Government infrastructure development?

3. Define key security challenges for government system? Explain an approach to security for e-Government

Group B

Answer SEVEN questions. **$7 \times 8 = 56$**

4. Explain the way of partnership followed by e-Government. Describe citizen-centric approach to c-Government adoption.

5. What are the issues in e-Government readiness? Explain different steps to e-Government readiness.

6. Describe emerging management issues for e-Government system.

7. Describe e-Government system life-cycle. Mention design of new e-Government system.

8. Explain e-Government strategy and managing public data for Government with an example.

9. What is GIDC? Show comparative analysis of c-Government development in India and China.

10. Explain different application areas of data warehousing and data mining in brief.

11. Write short notes on any TWO:

    (a) Security management model

    (b) e-Government master plan

    (c) ICT development project in Nepal

REFERENCES

Chaulagain, J. (2021). Important Questions and Answers of e-Governance: BCA-VIII. *Gomendra Multiple College*.

Satyanarayana, J. (2004). *E-government: The science of the possible*. PHI Learning Private Limited.

Heeks, R. (2006). *Implementing and managing egovernment*. Sage Publications Ltd.

S. Prabhu, & N.Venkatesan. (2007). *Data mining and warehousing*. New Age International (P) Limited, Publishers.

eGovernance. (2010). Retrieved January 22, 2021, from https://sarojpandey.com.np/academic/

Shah, N. K. (2017). eGovernance Notes. *Purbanchal University School Of Engineering & Technology*.

EGovernance Notes. (n.d.). Retrieved January 22, 2021, from http://bsccsitblog.blogspot.com/2015/04/e-governance-notes.html

General Overview of NITC/GIDC. (n.d.). Retrieved January 25, 2021, from https://nitc.gov.np/aboutus/introduction

E-Government Implementation Course Manual for High Level Officers of Nepal Government. (2015). National Information Technology Center - Disaster Recovery Center. 04 Huprachur, Hetauda, Makwanpur, Nepal (44107). Retrieved January 25, 2021, from https://drc.nitc.gov.np/assets/img/downloads/200812043542MODULE_I.pdf

About e-Suvidha. (n.d.). Retrieved February 12, 2021, from http://esuvidha.goup.in/about-e-suvidha

Mission & Vision. (n.d.). Retrieved February 12, 2021, from http://esuvidha.goup.in/mission-vision/