3

E-GOVERMENT INFRASTRUCTURE DEVELOPMENT

CHAPTER OUTLINE

After comprehensive study of this chapter, you will be able to:

- Network Infrastructure
- Computing Infrastructure
- Data Centers
- E-Government Architecture
- Interoperability Framework
- Cloud Governance
- E-readiness; Data System Infrastructure
- Legal Infrastructural Preparedness
- Institutional Infrastructural Preparedness
- Human Infrastructural Preparedness
- Technological Infrastructural Preparedness

E-Governance is the application of information and communication technologies (ICTs) to improve the activities of government agencies. Today, across the world governments are using several e communication strategies to effectively administer the public and private activities of which India is one of them.

A governance infrastructure is the collection of technologies and systems, people, policies, practices, and relationships that interact to support governing activities.

e-Governance Strategy' is an approach or a plan of action stating how Information Technology will be leveraged in achieving the stated goals and objectives.

Leverage: Using something valuable to achieve a desired result

E READINESS

E-readiness (electronic readiness) is defined as a degree to which to a country or economy may be ready, willing or prepared to obtain benefits which arise from information and communication technologies. This measure is often used to gauge how ready a country is to participate in electronic activities such as e-governance.

E-readiness also defined as "The degree to which a community is prepared to participate in the Networked World, which is gauged by accessing a community's relative advancement in the area that are most critical for ICT adoption and the most important of ICTs"

E-Readiness is the ability to use information and communication technologies (ICT) to develop one's economy and to foster one's welfare.

- Is a measure of e-business environment, a collection of factors that indicate how amenable (willing) a market is to Internet-based opportunities.
- Is not simply a matter of the number of computer servers, websites and mobile phones in the country, but also things such as its citizen's ability to utilize technology skillfully, the transparency of its business and legal systems, and the extent to which governments encourage the use of digital technologies.

Data System Infrastructure

The core of e-governance is e-MIS and holds the entire database of any organization.

- The major question that arises here is " Are all the requisite management information systems, records, databases and work processes in proper place so as to provide the quantity and quality of data to support the move to e-governance?"
- The data that were managed manually need to be computerized or brought into electronic form which means that the preparedness of computerized database or data warehouse is required.
- Data quality and data security are of prime concern here as most of the government infrastructures are not up to the mark in developing countries.
- This is the core computerization activity of any government process which may take several years to reach this stage.

Legal Infrastructure Preparedness

They lack requisite legislation and legal infrastructure to enable such reforms or reengineering of the existing business practices, rules and regulations within the government at various levels.

The manual processes in government are usually obsolete, inefficient and bureaucratic.

- Though they have transformed to computerization practices, they continue to have poor and inefficient performance and this is due to lack of administrative reforms and lack of business process reengineering.
- This seems to be accentuated in developing countries while developed countries have been significantly successful in administrative reforms and business reengineering.
- The fundamental question that arises here is " Are the laws and regulations required to permit and support the move towards e- governance initiatives in place?

  E.g Digital Signature Act

Institutional Infrastructural Preparedness

- For any government to implement a successful e-governance project, the required institutional infrastructure must be in place which most of the government lack.
- The government body has to establish a separate IT department which basically coordinates with facilitators for e-government projects within the nation.
- The IT department works out for the hardware selection and procurement, network or software development and implementation and also the training of staff at various levels of the government.
- Many countries still lack the institutional infrastructure.

Human Infrastructural Preparedness

- Human resource development by training is an essential requirement which comes from well trained manpower both technical and non-technical.
- The technical manpower resources are essential for all the phases of e- governance and related information system life cycle comprising systems analysis, design, programming, implementation, operation and documentation.
- Both private and government institutions should play a major role in this regard.
- Apart from technical human infrastructure, there is a need for the crucial training and orientation of user personnel i.e. government staff in e- governance project.
- The government employees and staff who are the stake-holders in all e-government projects as the end users are to be appropriately trained and oriented for change management from a manual government environment to e-governance environment.
- Such training will make them competent and capable of handling e- governance projects at operational level

Technological Infrastructural Prepaidness

Technology is fast changing in ICT domain and there is a rapid obsolescence of software as well as hardware which require great financial support time and again.

- Government organizations encounter this situation especially as their procedures to procure hardware or software are very inefficient and slow.
- The technological infrastructure in developing countries including computing and telecommunication is absent. As a result software and hardware may not be compatible.
- The major reasons are
- cost of technology
- Adaptability
- Obsolescence
- This is a serious limitation to e-governance implementation.

Need of E-Readiness

E-readiness is defined as the aptitude of an economy to use information and communication technologies to migrate traditional businesses into the new economy. E-readiness reaches its optimal level when the economy is able to create new business opportunities that could not be done otherwise. The concept of e-readiness is important because its level can be a strong predictor of how well a country can perform in the new economy. An e-readiness assessment would provide policy makers with a detailed scorecard of their economy's competitiveness relative to its international counterparts. Further, a breakdown of indicators allows policy analysts to pinpoint areas of strengths and weaknesses, thus providing a balanced perspective in guiding a country through the digital transformation.

NETWORK INFRASTRUCTURE

Network infrastructure is typically part of the IT infrastructure found in most enterprise IT environments. The entire network infrastructure is interconnected, and can be used for internal communications, external communications or both. A typical network infrastructure includes:

Networking Hardware

Networking hardware, also known as network equipment or computer networking devices, are electronic devices which are required for communication and interaction between devices on a computer network. Specifically, they mediate data transmission in a computer network.

1. **Routers**

   The router is a physical or virtual internetworking device that is designed to receive, analyze, and forward data packets between computer networks. A router examines a destination IP address of a given data packet, and it uses the headers and forwarding tables to decide the best way to transfer the packets.

2. **Switches**

A switch is a hardware device that connects multiple devices on a computer network. A Switch contains more advanced features than Hub. The Switch contains the updated table that decides where the data is transmitted or not. Switch delivers the message to the correct destination based on the physical address present in the incoming message. A Switch does not broadcast the message to the entire network like the Hub. It determines the device to whom the message is to be transmitted. Therefore, we can say that switch provides a direct connection between the source and destination. It increases the speed of the network.

3. **LAN cards**

A LAN card connects a computer to a network. LAN cards are typically built into your computer. You can connect to the network via an Ethernet cable, usb, or wirelessly. LAN cards also make it possible to connect many different computers together through the LAN.

4. **Hub**

A Hub is a hardware device that divides the network connection among multiple devices. When computer requests for some information from a network, it first sends the request to the Hub through cable. Hub will broadcast this request to the entire network. All the devices will check whether the request belongs to them or not. If not, the request will be dropped.

5. **Cables**

Network cables are used to connect and transfer data and information between computers, routers, switches and storage area networks. These cables are essentially the carrier or media through which data flows. There are different types of communications cables, and the appropriate type to use will depend on the structure and topology of the overall architecture of the system.

Networking Software

Networking software is a foundational element for any network. It helps administrators deploy, manage and monitor a network. Traditional networks are made up of specialized hardware, such as routers and switches that bundle the networking software into the solution.

1. **Network operations and management**

Network Operations. Management. Manage, Automate, and Ensure Compliance for Physical, Virtual, and Software-Defined Networks. It is the first heterogeneous network management solution to provide unified management for modern networks.

2. **Operating systems**

An operating system is the most important software that runs on a computer. It manages the computer's memory and processes, as well as all of its software and hardware. It also allows you to communicate with the computer without knowing how to speak the computer's language. Without an operating system, a computer is useless.

3. **Firewall**

A firewall is a system designed to prevent unauthorized access to or from a private network. You can implement a firewall in either hardware or software form, or a combination of both. Firewalls prevent unauthorized internet users from accessing private networks connected to the internet, especially intranets.

Network Services

A networking service is a low-level application that enables the network to perform more than basic functions.

1. **T-1 Line**

A T1 line is a communications transmission service that uses 2 twisted pair copper wires to transmit and receive data or voice traffic. A T1 line can transmit data at a speed of 1.544 Mbps.

2. **DSL**

Stands for "Digital Subscriber Line." DSL is a communications medium used to transfer digital signals over standard telephone lines. Along with cable Internet, DSL is one of the most popular ways ISPs provide broadband Internet access.

3. **Satellite**

A satellite is an object in space that orbits or circles around a bigger object. There are two kinds of satellites: natural (such as the moon orbiting the Earth) or artificial (such as the International Space Station orbiting the Earth).

4. **Wireless protocols**

Wireless communication protocols are used to connect computers, laptops and smartphones. The more widespread and standardized protocols are wireless LAN (IEEE 802.11) or Bluetooth (IEEE 802.15. 1). The implementation of these protocols in a device requires high processing capacity and big energy consumption.

5. **IP addressing**

An Internet Protocol address (IP address) is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. An IP address serves two main functions: host or network interface identification and location addressing.

COMPUTING INFRASTRUCTURE

Computing Infrastructure provides the hardware and services that other systems and services are built on. Computing Infrastructure provides management and support for end-user computers, servers, storage systems, operating systems, databases, middleware and ERP systems. There are three groups that make up the Computing Infrastructure team:

Database and ERP Administration

The Database and ERP Administration group manages and supports the main database infrastructure for core applications used by staff, faculty and students, based on Oracle Database software. It also manages and supports Oracle and MySQL databases for a variety of administrative and academic needs. In addition, it provides Microsoft SQL Server database support and assists with the integration of the SQL Server database with other third-party applications. The group is also responsible for installing, configuring, building and recovering processes, securing and monitoring the health of the database infrastructure.

End-User Computing

The End-User Computing group consists of two teams that provide personal computer management, support and assistance to faculty and staff, in addition to academic computer labs and classrooms management. The End-User Computing hardware team is the "hands and feet" for CCS. This team provides guidance, recommendations and assists faculty and staff with personal computer, printer, and other device acquisition needs. The team also provides personal computer operating system imaging and application setup and support, including hardware installation and connectivity to the network. In addition, the hardware team provides hardware troubleshooting and repairs of supported desktop, laptop and printer equipment used by faculty and staff, as well as support for equipment installed in labs or podiums managed by CCS and used by students and faculty. The End-User Computing infrastructure team provides back-end management and support for a number of key applications, including Microsoft Active Directory, used to provide authentication and rights access to services such as network shares and other services. This team is responsible for managing the printing infrastructure for administrative networked printers and academic/lab printers. In addition, the infrastructure team builds, tests, installs and manages desktop images deployed in CCS academic managed labs, as well as labs owned by other departments. The End-User Computing group, as a unit, works very closely with other groups within CCS and other departments, to ensure that the best solutions and services are delivered in a secure and manageable way.

Server & Storage Services

The Server and Storage Services group is responsible for the CCS managed data centers, servers and storage systems that provide infrastructure resources to applications and services used by staff, faculty and students. This group ensures that the UPS and HVAC solutions within the data centers are operating efficiently and coordinates any maintenance, repairs and changes with other groups within CCS or outside of CCS, including Facilities Management and Development. The Server and Storage Services group is responsible for optimizing the operations within the data center, including the power distribution from UPS systems to allow power redundancy sources to data center equipment, as well as efficient cooling within the data

center. The Server and Storage Services group is also responsible for establishing standard server and storage platforms and for the management of the hardware and software required to integrate these platforms to deliver an efficient, scalable and cost-effective infrastructure capable of supporting layered services that consume server and storage resources, including core applications such as RAMSS, Human Resources, Finance, Bright space by D2L, and various other services.

The Computing Infrastructure team has a vast collective set of skills and expertise in areas such as data center management, Storage Area Networks, desktop and server imaging, database administration and general troubleshooting skills, that can be leveraged by other groups at the University for advice and consultation.

Computing Infrastructure provides the hardware and services that other systems and services are built on.

- **File and disk storage services:** Information Services provides a number of file and disk storage services. These include file servers, file backup, long-term archive and ftp services. Some of these services are provided by Storage Area Networks (SANs).
- **Authentication and authorization:** Authentication is the means by which you log in and identify yourself. Authorization is the means by which a service determines whether an authenticated person should have access to a service.
- **Virtual hosting:** The virtual hosting service provides a managed platform for hosting Windows, Linux and Unix services on a highly resilient virtualization platform based on VMware.
- **Cloud computing services:** An Open Stack service to provide a platform to self-provision server infrastructure to support both researchers and development teams.

DATA CENTERS

Data centers are simply centralized locations where computing and networking equipment is concentrated for the purpose of collecting, storing, processing, distributing or allowing access to large amounts of data. They have existed in one form or another since the advent of computers.

In the days of the room-sized behemoths that were our early computers, a data center might have had one supercomputer. As equipment got smaller and cheaper, and data processing needs began to increase -- and they have increased exponentially -- we started networking multiple servers (the industrial counterparts to our home computers) together to increase processing power. We connect them to communication networks so that people can access them, or the information on them, remotely. Large numbers of these clustered servers and related equipment can be housed in a room, an entire building or groups of buildings. Today's data center is likely to have thousands of very powerful and very small servers running 24/7.

Need of Data Center

Despite the fact that hardware is constantly getting smaller, faster and more powerful, we are an increasingly data-hungry species, and the demand for processing power, storage space and information in general is growing and constantly threatening to outstrip companies' abilities to deliver.

Any entity that generates or uses data has the need for data centers on some level, including government agencies, educational bodies, telecommunications companies, financial institutions, retailers of all sizes, and the purveyors of online information and social networking services such as Google and Facebook. Lack of fast and reliable access to data can mean an inability to provide vital services or loss of customer satisfaction and revenue.

What are the core components of a data center?

Data center design includes routers, switches, firewalls, storage systems, servers, and application delivery controllers. Because these components store and manage business-critical data and applications, data center security is critical in data center design. Together, they provide:

Network infrastructure. This connects servers (physical and virtualized), data center services, storage, and external connectivity to end-user locations.

Storage infrastructure. Data is the fuel of the modern data center. Storage systems are used to hold this valuable commodity.

Computing resources. Applications are the engines of a data center. These servers provide the processing, memory, local storage, and network connectivity that drive applications.

How do data centers operate?

Data center services are typically deployed to protect the performance and integrity of the core data center components.

Network security appliances. These include firewall and intrusion protection to safeguard the data center.

Application delivery assurance. To maintain application performance, these mechanisms provide application resiliency and availability via automatic failover and load balancing.

What are the standards for data center infrastructure?

The most widely adopted standard for data center design and data center infrastructure is ANSI/TIA-942. It includes standards for ANSI/TIA-942-ready certification, which ensures compliance with one of four categories of data center tiers rated for levels of redundancy and fault tolerance.

- **Tier 1:** Basic site infrastructure. A Tier 1 data center offers limited protection against physical events. It has single-capacity components and a single, non redundant distribution path.

- **Tier 2:** Redundant-capacity component site infrastructure. This data center offers improved protection against physical events. It has redundant-capacity components and a single, non redundant distribution path.
- **Tier 3:** Concurrently maintainable site infrastructure. This data center protects against virtually all physical events, providing redundant-capacity components and multiple independent distribution paths. Each component can be removed or replaced without disrupting services to end users.
- **Tier 4:** Fault-tolerant site infrastructure. This data center provides the highest levels of fault tolerance and redundancy. Redundant-capacity components and multiple independent distribution paths enable concurrent maintainability and one fault anywhere in the installation without causing downtime.

E-GOVERNMENT ARCHITECTURE

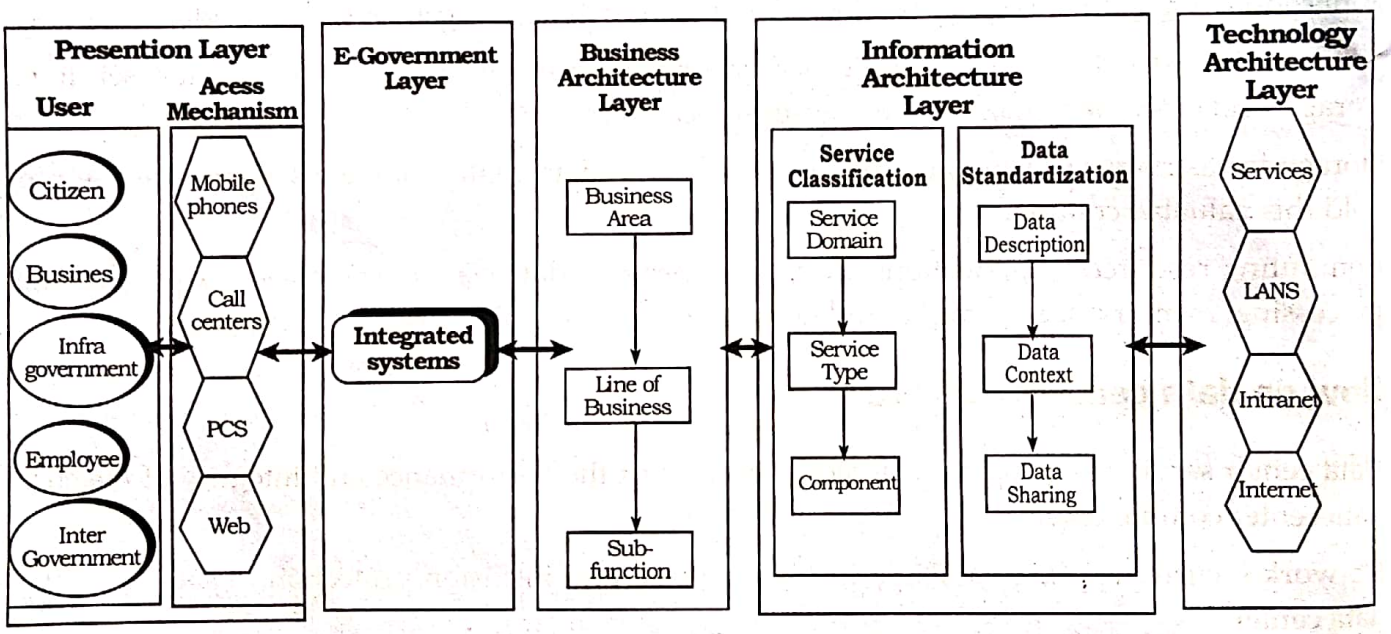

Fig: Overall E-Government architecture structure

Presentation Layer

The presentation layer identifies and describes the system users, who require access to government information at different capacities, and the channels through which information can be accessed. During system development, one is required to explicitly identify the government user, the system is intended to serve and also the means through which this information is to be accessed, so that the system can be tailored to meet these requirements.

It manages the user's interface with the system. If a project is to be successful, different stakeholders need to be identified in the beginning, involved in the initial stages, and kept involved throughout development and implementation.

E-Government Layer

E-government public services utilize very specialized applications those are only available to certain agencies and not all agencies participating in the consortium. The main goal of e-government layer is to achieve a government that;

- does not ask for information it already has
- Is focused on better services towards
- counties and national governments
- Will not allow its facilities to be misused
- Is well informed
- Is efficiently organized and in control of its internal affairs.

According to the Kenyan E-government architecture; with databases only in place semantic interoperability could not be realized due to the coherence between semantics within a more decentralized approach. This has been the greatest hindrance on the initial e-government initiatives; since public agencies develop their own systems independently from each other, and the granularity of how information is expressed differ greatly thus making seamless information flow a nightmare. Semantic interoperability should be at the core on all levels between databases and documents, processes and life events as can be seen in the subsequent layers. Therefore, E-government layer is the Culmination of the one source point of truth between the integrated national and county services.

Business Architecture Layer

The first-step toward a successful e-governance initiative is process re-engineering. This aims to simplify the existing processes and procedures, reduce the manual touch points and make the entire transaction cycle friendly. For E-governance to succeed, it is imperative that processes are simplified and understood by all stakeholders. The business layer provides a functional rather than organizational view of the government's lines of business; including its internal operations and services for citizens, independent of the agencies, bureaus and offices performing them. The business layer describes the devolved government around common business, thus promotes agency collaboration and serves as the underlying foundation for government process redesign and e-government strategies. Each business function is analyzed for potential for streamlining in order to facilitate optimization via collaboration and sharing. The whole government agrees on which domains there are to uniquely identifiable and how they are going to identify them. Both governments need to decide to which domain their process relates. Also, analysis of processes that might be affected or need to be integrated with legacy systems for efficient delivery of services, thus in this layer it not only touches organizational interoperability but also semantic and more insight to technical.

Information Architecture Layer

This layer can be divided into two; Service classification sub-layer; The service classification sub-layer classifies service components according to how they support business and performance objectives e.g. ERPS, CRMs. It serves to identify and classify horizontal and vertical service components supporting government and their IT investments and assets. It is organized across horizontal service areas independent of the business functions, providing a leverage able foundation for reuse of applications, application capabilities and business services.

Data Standardization Sub-layer

The data standardization sub-layer is flexible and standard based to enable information sharing and reuse across the government via the standard description and discovery of common data and the promotion of uniform data management practices. It provides a standard means by which data may be described, categorized and shared. These are reflected within each of the three standardized areas;

Data descriptions

Data descriptions, provides a means to uniformly describe data, thereby supporting its discovery and sharing.

Data context

Data facilitates discovery of data through an approach to the categorization of data according to taxonomies.

Data sharing; Data sharing, supports the access and exchange of data; where access consists of ad hoc requests (such as a query of data access asset) and exchange consists of fixed, recurring transactions between parties, enabled by capabilities provided by both the data context and data description standardization areas.

It provides guidance for implementing repeatable processes to enable data sharing in accordance with government-wide agreements encompassing national, county as well as other public and private non-governmental institutions. The intent is to mature, advance and sustains their data agreements in and iterative manner.

Technology Architecture Layer

The technology architecture layer categorizes the standards and technologies that support and enable the delivery of service components and capabilities. It also unifies existing agency technologies and e-government guidance by providing a foundation to advance the reuse and standardization of technology and service components from a government wide perspective.

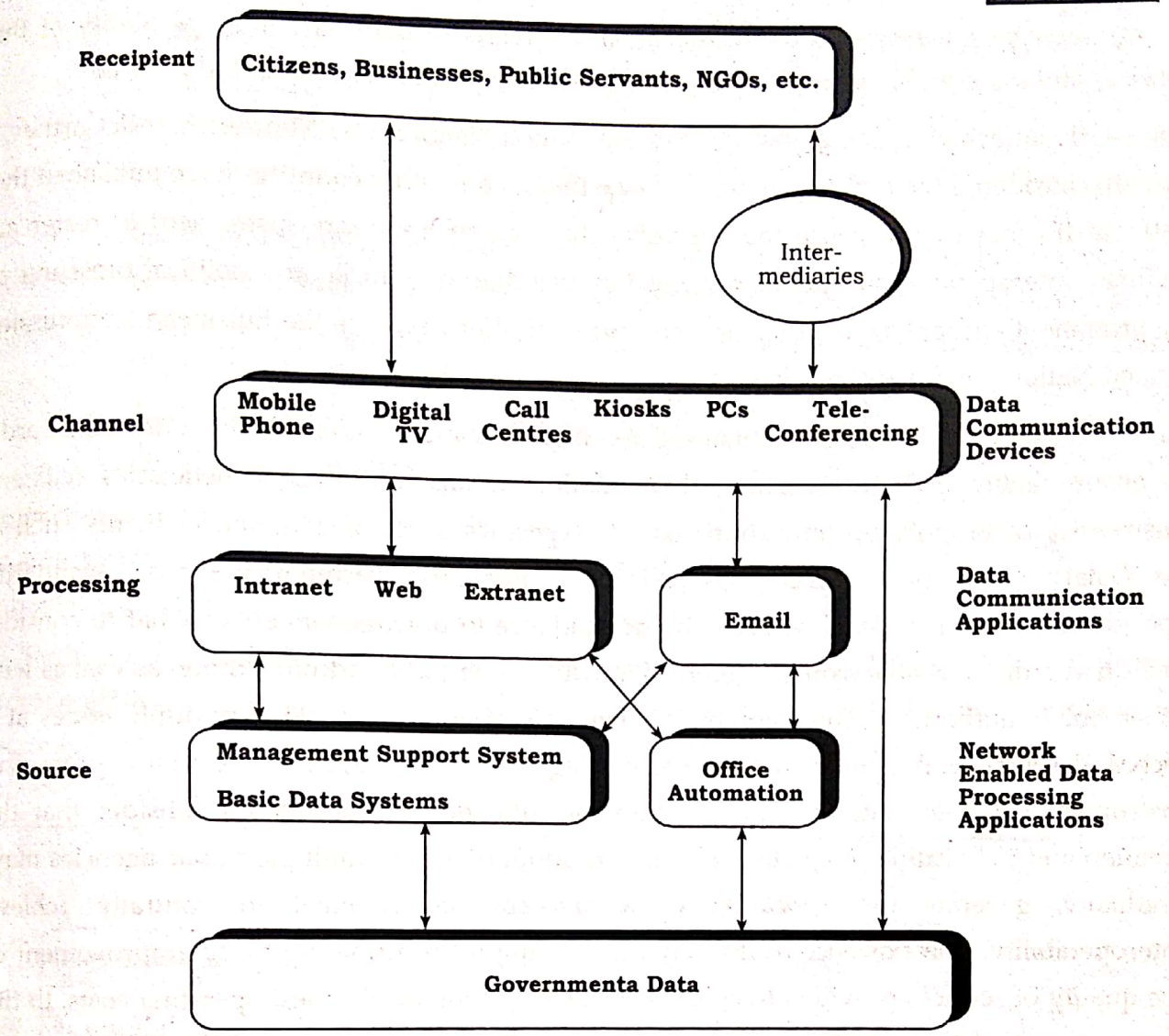

Fig:: Architecture of an E-governance

INTEROPERABILITY FRAMEWORK

Interoperability Framework is Set of standards and guidelines which describe the way in which organizations have agreed, or should agree, to interact with each other.

First Definition

E Government Interoperability Framework (eGIF) is a set of guidelines and standards to be followed by public sector information systems and processes, in order to achieve technical, organizational and semantic interoperability during service provision.

Second Definition

An e-government Interoperability Framework (IF) is a document or group of documents that specify a set of common elements such as vocabularies, concepts, principles, policies, guidelines, recommendations, standards, and practices for agencies that wish to work together, towards the joint delivery of public services.

IFs are seen by governments as promising instruments to boost the interoperability of their services and systems. Henceforth, many countries have created and published their Ifs.

The e-GIF, launched in September 2000 in the United Kingdom by Minister Ian McCartney, is usually considered the first IF published. Since then, many other countries have published their national IFs, not only because they perceive them as an important instrument to foster and facilitate interoperability of public systems but also due to financial and political pressures set by prominent and powerful organizations and institutions such as the European Commission, United Nations, and the World Bank.

An IF is "a strategic document containing specifications and standards to be followed in order to ensure interoperability among public administrations and their beneficiaries (citizens, businesses, other public administrations)". It "specifies a set of common elements such as vocabulary, concepts, principles, policies, guidelines, recommendations, standards, specifications and practices", which provide guidance to practitioners about what to consider and do in order to enable seamless interaction within their public administration as well as with other public authorities. The common elements set in an IF may cover multiple issues at a technical, semantic, organizational, or even at a legal or political level. IFs are seen as promising instruments to boost interoperability. Many practitioners and academics consider that the creation and publication of a national IF and its adoption by the multiple public agencies may, gradually, generate the appearing of a favorable environment to naturally achieve interoperability. The existence of IFs may thus ending up contributing to the improvement of the quality of services provided to citizens, to the reduction of agencies' operating costs, to the improvement of the coordination of government agency programs, and to the increase of transparency and accountability of government.

Interoperability Framework for E-Governance

IFEG in Indian context would encompass agreed approach to be adopted by the public agencies that wish to work together towards the joint delivery of public services using ICT, to achieve above mentioned goals, namely exchange of data, meaning of exchanged data and agreed process. An IFEG involves a common structure which comprises a set of standards and guidelines; the structure can be used by the public agencies to specify the preferred way that all stake-holders interact with each other to share the information. It is synonymous to speaking a common language.

Levels of Interoperability

The interoperability levels related to the sharing of information in IFEG are mainly classified into:

- Organizational Interoperability (like process-re-engineering including Government-Orders, Process Changes, Organizational Structures), Semantic Interoperability (Enabling data to be interpreted & processed with the same meaning, etc.) and
- Technical Interoperability (like technical issues in interconnecting ICT systems and services, information storage and archival, protocols for information exchange and networking, security, etc.); in general, technical interoperability was considered for classifying the standards into various layers or domains (eg. Presentation domain, Network domain, Data Interchange domain, etc.) in earlier versions of IFEG/GIF documents from various countries.

Figure provides an overall view of the levels of the interoperability system. This helps to define the way in which applications and re-usable services will be developed and their interaction with other ICT systems.

As indicated in the Figure, Organizational Interoperability is supported by Semantic Interoperability, which in turn is supported by Technical Interoperability. Hence Technical Interoperability forms the basis for the IFEG. Governance facilitates and enforces the implementation of IFEG.

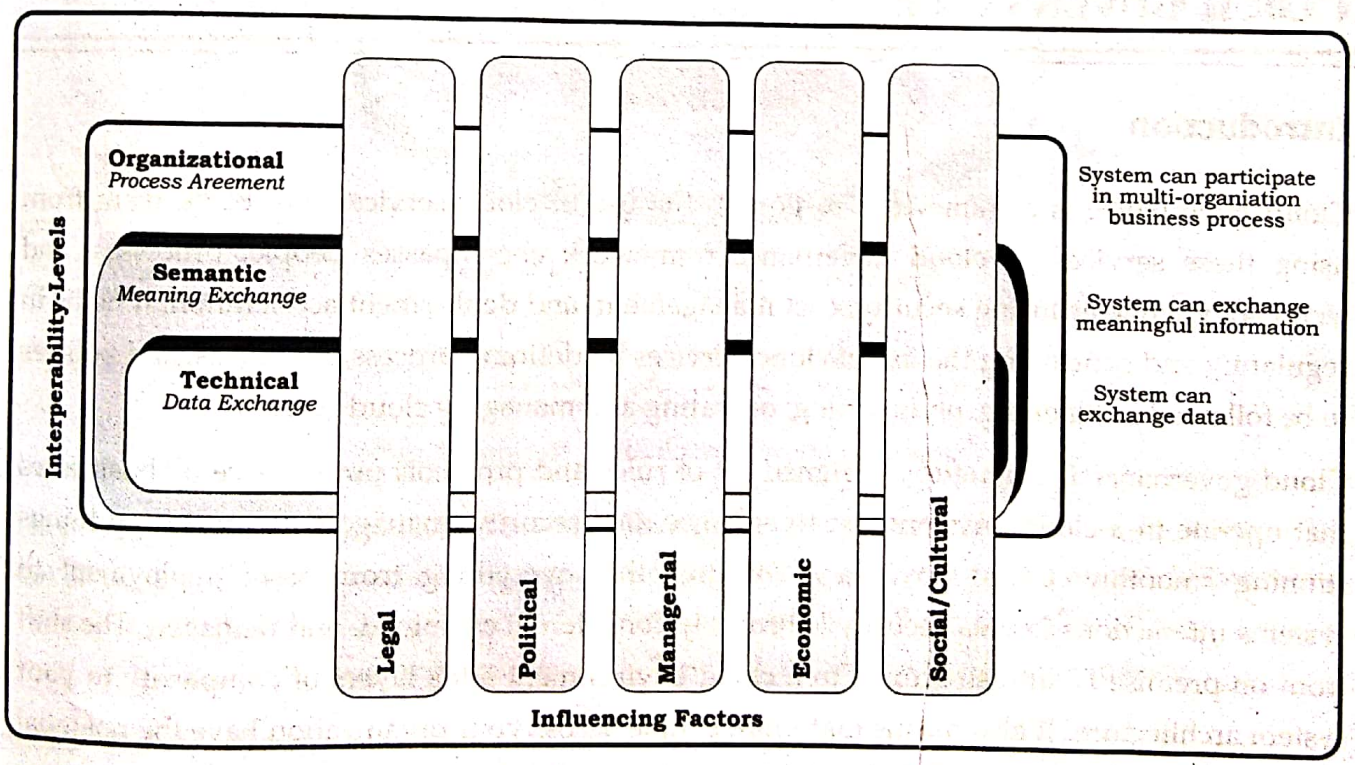

Figure: E-Governance Interoperability Model

The Multilateral mechanism for IFEG is influenced by the following key sub-areas:

- **Political**: For strategy related issues. In Political context, support and commitment from authority, provisioning of policies / guidelines, strategies over different levels of interoperability are expected.

- **Legal:** For issues like IPR / Copy Right, content regulation, privacy, freedom of information, electronic identities, etc; these are context-sensitive. Legal factors include legal-power assigned to system for data protection and privacy information of the citizen, governance issues related to information management, executive orders and laws related to e-Governance services, citizen services driven by administrative procedures, enforcement, etc.
- **Managerial:** For issues like training, motivation, reorientation of concerned staff from public agencies.
- **Economic:** For funding related issues.
- **Social/Cultural:** For social/cultural characteristics of system stakeholders. Social / Cultural factors like differences in culture, working practices, issues of trust, timings, social exclusion issues have more influence. Cultural and linguistic diversity in India introduces additional administrative constraints like naming conventions, multiple local official languages, language dependent format, etc.

CLOUD GOVERNANCE

Introduction

Cloud governance is a framework to govern the use of cloud services, not block them from using these services. A cloud governance framework encompasses people, processes, and technology while ensuring security, cost management, and deployment acceleration. It helps in regulating and controlling the use of cloud services by defining process, standards, and policies to be followed in planning, on-boarding, operating and managing cloud services.

Cloud governance is a carefully designed set of rules and protocols put in place by businesses that operate in a cloud environment to enhance data security, manage risks, and keep things running smoothly. Cloud governance ensures that everything from asset deployment to systems interactions to data security is properly considered, examined, and managed. The shift from on-premise IT infrastructures to a cloud environment adds layers of complexity to your system architecture. It also means that more people across your organization have the potential to impact that architecture. This is why it's critical to develop and maintain a comprehensive cloud governance model.

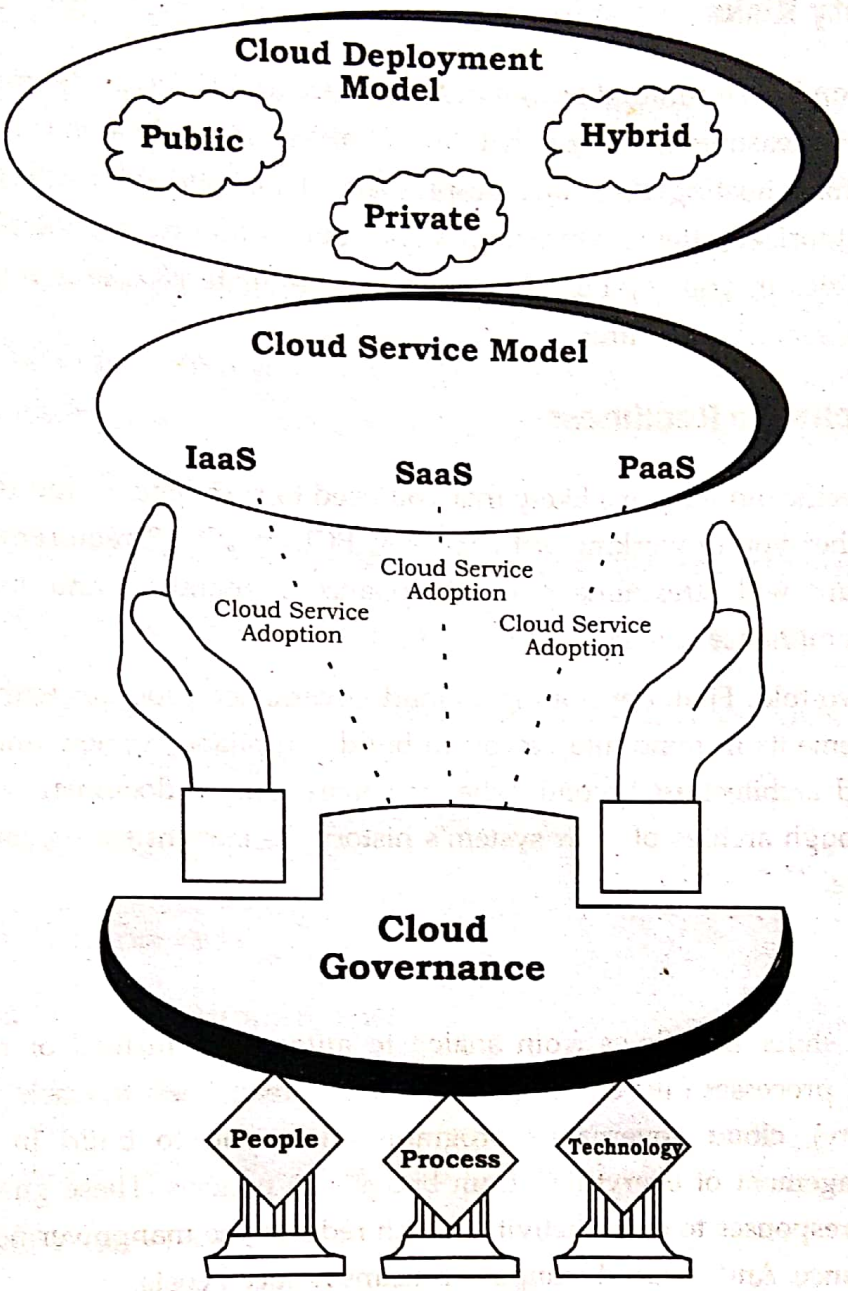

Fig: Benefits of a cloud governance framework

Designing and implementing a best-in-class cloud governance framework takes time and effort. It's not something that can be pulled together in an afternoon, and you'll need to collaborate across teams to ensure that the final product is complete and actionable. But it's worth it. When developed properly, your cloud governance framework will return immediate and long-term benefits.

Controlled Access

By designating who owns each area of asset and software management, your cloud governance plan will build necessary limits on who can access and impact your cloud ecosystem. As mentioned earlier, this is especially important considering how easy it is to implement new assets to the cloud. The last thing you want is rogue IT applications and initiatives tampering with your sensitive architecture. Controlling access to critical assets is vital and will enhance the reliability of your cloud processes.

Reduced Security Risks

Once an organization has committed to moving their data to the cloud, it's imperative that they develop the security measures to protect that data. While housing data on the cloud is certainly more convenient than hosting that data on-premise, it also brings increased risk for data breaches and unauthorized attempts to access data. Your cloud governance plan will help you identify vulnerabilities in your system, enact plans to mitigate risk, and establish metrics to gauge the impact of security measures.

Enhanced Compliance Readiness

No matter your specific industry, it's likely that you need to pass regular audits and compliance assessments. Whether you're working with HIPAA, PCI, or SOC 2 requirements, your cloud governance program will streamline your compliance preparation and make it easier to demonstrate that compliance.

The benefits are two-fold. First, developing a cloud governance program with your particular compliance requirements in mind allows you to build compliance review and standards into your processes and architecture. Second, when it comes time to document your compliance, you'll have a thorough archive of your system's history, its current status, and your plans to enhance compliance.

Lowered Costs

Cloud governance shifts workflows from analog to automated. Instead of relying on time-consuming manual processes (like crafting complicated spreadsheets to track various accounts and system activity), cloud governance programs allow you to build in guardrails that automate the management of everything from budgets to policies. These guardrails can also trigger automated responses to cloud activity, which reduces the manpower needed to enforce your cloud governance. And reduced manpower means reduced costs.

Establishing Cloud Governance

Cloud governance is established in the following three phases described in the table below.

Plan	Build	Operate and Manage
• Define vision and scope	• Define reference architecture	• Monitor
• Define service catlog	• Setup/configure tool	• Measure KPI
• Define government framework & tool	• Build governance organization	• Optimize
• Define KPIs to measure the effectiveness of cloud governance	• Define standards, templates, policies and procedures	

Elements of Cloud Governance

Cloud Governance is comprised of the following key components.

- Cloud Business Office (CBO) ensures alignment of cloud vision with business vision and ensures that governance is enforced across the enterprise. CBO is also responsible for demand management, cost optimization, and prioritization.
- Cloud CoE (Center of Excellence), which is a cross-functional team that defines processes, regulates and standardize cloud adoption, migration and operation across the enterprise.
- Cloud governance organization structure and roles and responsibilities
- Cloud governance processes around the cloud service lifecycle
- Cloud foundational components like cloud reference architecture, standards, templates, guidelines, best practices and policies

Risk of Poor Cloud Governance

- Cloud Security Risks
- Cloud Proliferation and Sprawl
- Cloud Integration (post proliferation)
- Cloud Portability & Interoperability
- Cloud Vendor Lock-In
- Cloud Applications Governance - designing and migrating applications to appropriate Cloud pattern(s)
- Lack of Incentives for Consumers to Onboard/Consume Cloud resources
- Shadow IT and Hidden Clouds

DISCUSSION EXERCISE

1. Define E readiness. Explain in brief about infrastructural prerequisite of e readiness.
2. Write short notes:
   a. Legal infrastructural preparedness
   b. Technology infrastructure preparedness
3. Explain E government architecture with a proper diagram.
4. What is Cloud Governance ? Explain its importance .
5. Explain Interoperability Framework with a proper diagram. What are the benefits of Interoperability Framework.
6. What is Data Centers and also discuss its importance. In there any Data Center in Nepal. Explain of any ?
7. Write short notes on:
   a. Network Infrastructure
   b. Computing Infrastructure
   c. Data Center
8. Discuss human infrastructural preparedness for e governance.
9. E-governance evolves gradually from simplest level to advanced level. justify
10. Discuss the steps to E governance readiness.

❑❑❑