Unit 3

Unit 3: E-Governance Infrastructure, Stages in Evaluation and Strategies for Success (8 Hrs.)

E-readiness - Data System Infrastructure, Legal Infrastructural Preparedness, Institutional Infrastructural Preparedness, Human Infrastructural Preparedness, Technological Infrastructural Preparedness; Evolutionary Stages in E-Governance

E-readiness

- ✓ E-readiness refers to the level of preparedness of a country, region, or organization to adopt and utilize information and communication technologies (ICTs), including the internet and digital technologies, for development and governance purposes.

- ✓ E-readiness is often used to assess the potential for a country or region to implement and benefit from e-governance initiatives, e-commerce, and other forms of digital transformation.

Developing countries face serious constraints and limitations or challenges to fully adopt e-governance. All these are related to the e-readiness of the country i.e. its readiness for e-governance implementation. E--readiness means the infrastructural pre-requisites for taking up any e-governance initiative. These infrastructural prerequisites or preconditions may be

identified as:

- Data System Infrastructure Preparedness
- Legal Infrastructural Preparedness
- Institutional Infrastructural Preparedness
- Human Infrastructural Preparedness
- Technological Infrastructural Preparedness
- Leadership and strategic planning

Data System Infrastructure Preparedness

- Data system infrastructure preparedness refers to the level of readiness of an organization or government to implement and manage a robust and secure data system infrastructure to support its operations and goals.

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

- The data that were managed manually need to be computerized or brought into the electronic form which means that the preparedness of a computerized database or the data warehouse is required.

- The major question that arises here is **"Are all the requisite management information systems, records, databases, and work processes in the proper place so as to provide the quantity and quality of data to support the move to e-governance?"**

A data system infrastructure that is well prepared includes the following components:

IT infrastructure: This includes the hardware, software, and network systems that are required to support the organization's data system.

Data management systems: The organization must have robust data management systems in place, including data storage, backup, and recovery systems.

Data security systems: The organization must have robust security systems in place to protect its data from unauthorized access and ensure the confidentiality, integrity, and availability of its data.

Data governance framework: The organization must have a clear data governance framework in place to ensure that its data is used ethically and in compliance with legal and regulatory requirements.

Skilled workforce: The organization must have a trained and skilled workforce that is capable of managing and maintaining its data system infrastructure.

▸ Data system infrastructure preparedness is critical to the success of any organization or government, as it supports the effective use of data for decision-making, planning, and service delivery. By investing in a well-prepared data system infrastructure, organizations and governments can improve the accuracy, quality, and availability of their data, and support more effective and efficient operations and decision-making processes.

Legal infrastructural preparedness

- Legal infrastructural preparedness refers to the level of readiness of a country, region, or organization to have in place the legal and regulatory frameworks that support the effective implementation of information and communication technologies (ICTs) and e-governance initiatives.

- Though they have transformed to computerization practices, they continue to have poor and inefficient performance and this is due to a 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?"**

A legal infrastructure that is well prepared includes the following components:

Legal framework for ICTs: This includes laws and regulations that support the use of ICTs, protect the rights of citizens and businesses in the digital space, and address issues such as data privacy, security, and intellectual property rights.

E-governance laws: The country or region must have laws and regulations in place that support the implementation of e-governance initiatives, including laws that regulate the use of digital signatures, electronic transactions, and other digital technologies in governance processes.

Cyber security laws: The country or region must have laws in place to address cybercrime, cyberwarfare, and other cyber security threats.

Data protection laws: The country or region must have laws in place to protect the privacy and security of personal and sensitive information, and to regulate the use of such information by government and other organizations.

Institutional Infrastructural Preparedness

- ✓ Institutional infrastructural preparedness refers to the level of readiness of a government or organization to have in place the institutional structures and capacities that are needed to support the effective implementation of information and communication technologies (ICTs) and e-governance initiatives.

- ✓ For any government to implement a successful e-governance project, the required institutional infrastructure must be in place which most of the government lacks.

- ✓ The government body has to establish a separate IT department that 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 staff training at various levels of the government.

- ✓ Many countries still lack the institutional infrastructure

An institutional infrastructure that is well prepared includes the following components:

▸ **Institutional structure**: The government or organization must have a clear and well-defined institutional structure that is responsible for the implementation and management of ICTs and e-governance initiatives.

▸ **Technical capacities**: The government or organization must have in place the technical capacities and skills required to effectively implement and manage ICTs and e-governance initiatives, including expertise in areas such as ICT infrastructure, data management, and cyber security.

▸ **Organizational culture**: The government or organization must have a culture that values and supports the use of ICTs and e-governance initiatives, and that is committed to continuous improvement in this area.

▸ **Partnerships and collaborations**: The government or organization must be able to effectively collaborate and partner with other organizations and stakeholders, including private sector organizations and civil society groups, to support the implementation and sustainability of ICTs and e-governance initiatives.

Human infrastructural preparedness

Human infrastructural preparedness refers to the level of readiness of a country, region, or organization to have in place the human resources and capacities that are needed to support the effective implementation of information and communication technologies (ICTs) and e-governance initiatives.

A human infrastructure that is well prepared includes the following components:

▸ **Skilled workforce**: The country, region, or organization must have a trained and skilled workforce that is capable of implementing and managing ICTs and e-governance initiatives, including expertise in areas such as ICT infrastructure, data management, and cyber security.

- **Human resources management**: The country, region, or organization must have effective human resources management systems in place to support the recruitment, development, and retention of a skilled workforce.

- **Education and training**: The country, region, or organization must have strong education and training systems in place to support the development of a skilled workforce and to ensure that workers are able to keep pace with advances in technology and e-governance practices.

- **Public awareness and participation**: The country, region, or organization must have strong public awareness and participation programs in place to educate citizens and businesses about the benefits and opportunities of ICTs and e-governance initiatives, and to encourage their active involvement in these initiatives.
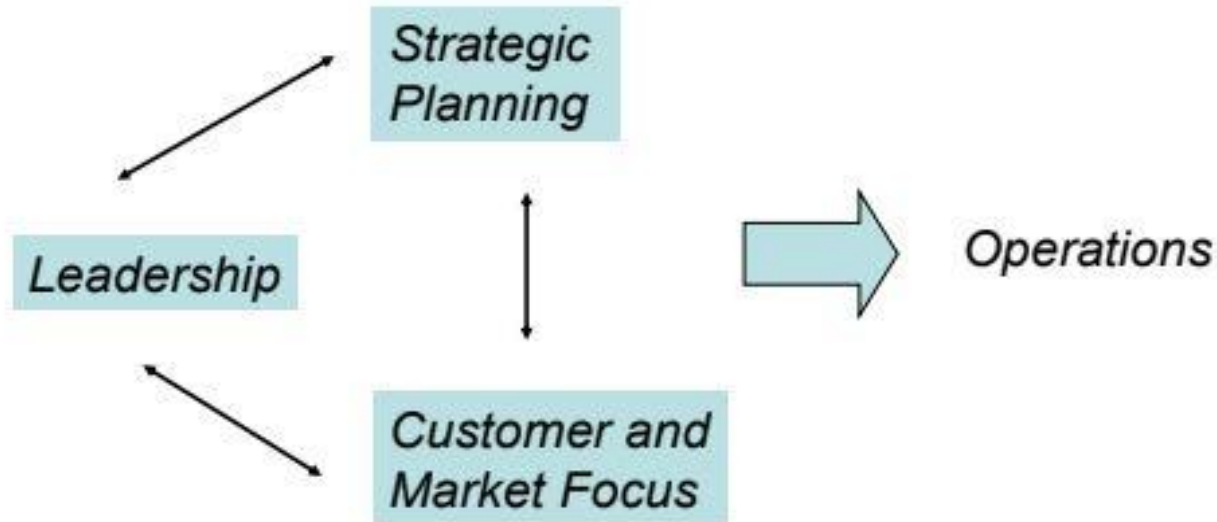
Technological infrastructural preparedness

▸ Technological infrastructural preparedness refers to the level of readiness of a country, region, or organization to have in place the technological resources and capacities that are needed to support the effective implementation of information and communication technologies (ICTs) and e-governance initiatives.

▸ A technological infrastructure that is well prepared includes the following components:

▸ **ICT infrastructure:** The country, region, or organization must have a robust and reliable ICT infrastructure in place, including telecommunications networks, data centers, and other critical components that are needed to support e-governance initiatives.

▸ **Technology standards:** The country, region, or organization must have in place clear and consistent technology standards that support the interoperability and integration of ICT systems and e-governance initiatives, and that promote the development of a sustainable technology ecosystem.

- **Cyber security:** The country, region, or organization must have strong cyber security measures in place to protect the confidentiality, integrity, and availability of information and systems, and to reduce the risk of cyber-attacks and other security incidents.

- **Technology innovation:** The country, region, or organization must be committed to continuous technology innovation and development, and must be able to effectively leverage new technologies and approaches to support the development and implementation of e-governance initiatives.
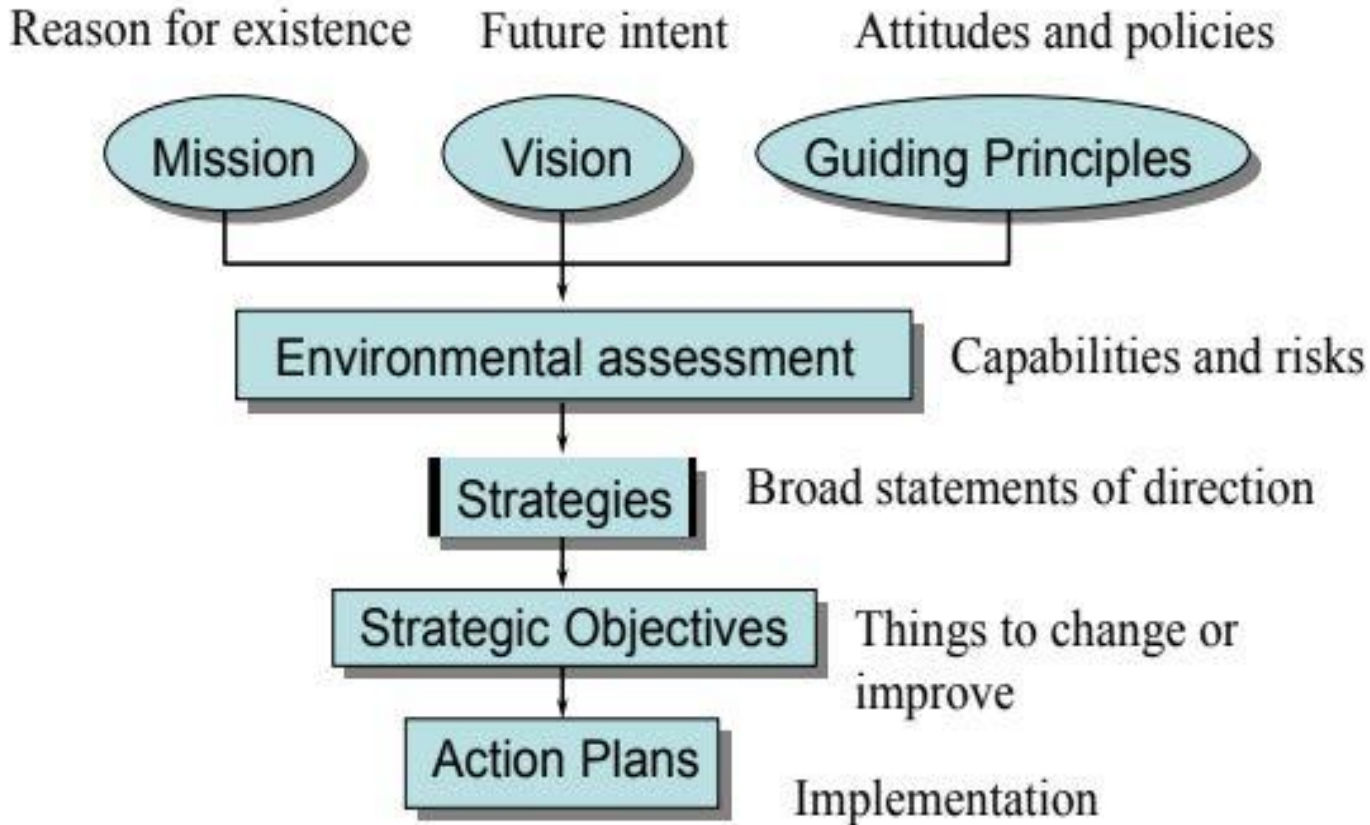
Leadership and strategic planning

Leadership

– The ability to positively influence people and systems to have a meaningful impact and achieve results.

– **Strategic Planning**

– The process of envisioning an organization's future and developing the necessary procedures and operations to achieve that future.

Strategic Planning Process

Reason for existence   Future intent   Attitudes and policies

Mission   **Vision**   **Guiding Principles**

Environmental assessment   Capabilities and risks

Strategies   Broad statements of direction

Strategic Objectives   Things to change or improve

Action Plans   Implementation

Evolutionary Stages in E-Governance

E-governance evolves gradually from the simplest levels to advanced levels and the evolution may not be same in all cases.

Stage 1: Use of e-mail and setting up of internal network

- The most fundamental, cheapest and easiest ICT tool is e-mail.
- Official orders to accept e-mail communication as valid have been issued in a large number of government, judicial and legislative organizations.
- Although e-mail can reach outside organizations via the Internet, most government organizations adopt e-mail for internal messaging.
- E-mails break the official hierarchy of communication, as anyone can send to e-mail to any other, breaking the hierarchy and other barriers.
- They allow person-to-person communication can improve information sharing, exchange, coordination and feedback of information.

Stage 2: Creation of intranets infrastructure for access of internal activities

An intranet infrastructure is a private network within an organization that provides access to information and resources for employees.

Stage 3: Allowing public access to information through Internet

Stage 4: Allowing two-way interactive communication with stakeholders to enable Internet enabled transactions (including financial transactions)

Stage 5: Allowing online transactions by the citizens

Enabled to make payments of fees and taxes, lodge complaints, file applications and perform any other transactions online through citizen.

Stage 6: Enriching digital democracy

- Democracy can be strengthened and enriched by ICT in multiple ways and modes.

- Digital democracy refers to the use of technology, such as the Internet and social media, to enhance and increase participation in the democratic process.

- This can include activities such as online voting, electronic petitions, and the use of social media to engage with elected officials and other political leaders.

Stage 7 Electronically integrated or joined government with Legislature and Judiciary.

▶ An electronically integrated or joined government refers to a system in which the executive, legislative, and judicial branches of government are connected and work together seamlessly through the use of technology.

▶ This can involve the use of electronic systems for communication, data sharing, and collaboration between the different branches of government, as well as the use of technology to increase the transparency and accessibility of government processes.

THANK YOU !

Compiled By:Er.Omkar Nath Gupta
nath.omkara@gmail.com