

UNIT 3

E-Governance Infrastructure, Stages in Evaluation and Strategies for Success

(8 Hours) — E-Governance (CACS409)

⚠ Please Note — May Contain Errors

These notes were prepared with AI assistance and **may contain errors, omissions or outdated information** (names, dates, figures, acronyms and project details in particular). Please take care: cross-check everything against your prescribed textbook, class notes and official sources before relying on it for exams or assignments.

3.1 E-Readiness

E-readiness is the degree to which a government, society or organisation is prepared to benefit from ICT and to carry out e-governance successfully. Before launching major e-governance projects, a country must check whether the foundations exist. Assessing e-readiness shows the strengths and weaknesses and helps in setting priorities, so that scarce funds are not wasted on projects that cannot succeed.

E-readiness is usually studied under five infrastructural headings: **data systems, legal, institutional, human and technological** preparedness.

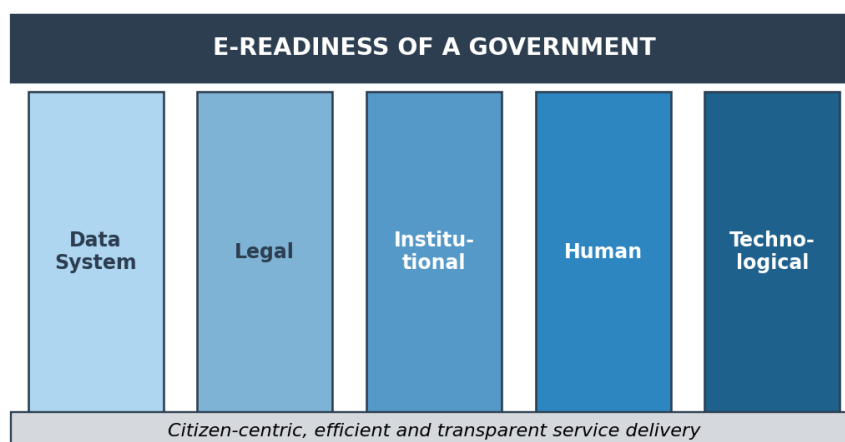


Figure 3.1 — Five pillars of E-readiness

1. Data System Infrastructure

E-governance depends on **accurate, complete and well-organised data**. Governments hold huge amounts of data (land records, citizens, taxes, licences, census) which is often on paper, duplicated or inconsistent. Data-system readiness means that data is digitised, standardised, secure and shareable.

- Digitisation of legacy records and creation of reliable databases / registries.
- Common data standards, codes and formats so that different departments can exchange data (interoperability).
- Data quality: accuracy, timeliness, completeness and removal of duplicates.
- Data security, backup, privacy protection and access control.
- Central facilities such as data centres, disaster-recovery site and data-sharing platforms.

2. Legal Infrastructural Preparedness

Electronic processes must have the **same legal standing** as paper ones. Laws and regulations are required to make online transactions valid, to protect users and to punish misuse.

- Legal recognition of electronic records, e-signatures and e-contracts (e.g. Electronic Transactions Act).
- Cyber-crime laws, data-protection and privacy laws, intellectual-property protection.
- Right to information laws, e-procurement and e-payment rules.
- Review and amendment of old laws and procedures that require paper or physical presence.
- Rules for certifying authorities, digital certificates and evidence admissibility in court.

3. Institutional Infrastructural Preparedness

Institutions must exist to **plan, coordinate and run** e-governance programmes. Without clear responsibility and leadership, projects remain scattered and incompatible.

- A lead agency or ministry for ICT policy, standards and coordination (e.g. a Department of IT / national IT centre).
- Strong political commitment and top-level leadership (a “champion”).
- Inter-departmental coordination bodies and clear roles for federal, provincial and local levels.
- Business-process re-engineering (BPR) and simplification of procedures.
- Project-management capacity, monitoring and evaluation, and a sustainable funding model, including public–private partnership (PPP).

4. Human Infrastructural Preparedness

Technology works only when **people** are able and willing to use it. Both government staff and citizens need skills and awareness.

- ICT training and capacity building for public servants at all levels.
- Availability of IT professionals (system analysts, developers, network and security experts) in or for government.
- Digital literacy among citizens and awareness of available services.
- Change management: reducing resistance and fear of job loss; incentives for adoption.
- Inclusion — language, gender, disability and rural-urban gaps.

5. Technological Infrastructural Preparedness

This is the **physical and technical base**: devices, networks, power and software platforms needed to run applications.

- Telecommunication and broadband networks reaching districts, local governments and villages (including mobile and optical fibre).
- Reliable electricity and alternative power; computers and end-user devices in offices.
- Government network (intranet / WAN), data centre, cloud and hosting facilities.
- Software platforms, databases, e-forms, payment gateways, portals and mobile apps.
- Standards, interoperability frameworks and cyber-security tools (firewalls, PKI, authentication).

Pillar	Question to ask	Example indicator
Data system	Is the data digital, clean and shareable?	% of records digitised
Legal	Are e-transactions legally valid and protected?	Existence of IT, privacy and e-signature laws
Institutional	Who plans, leads and coordinates?	Lead agency, master plan, budget
Human	Do people have the skills and willingness?	ICT-trained staff, literacy rate
Technological	Are networks, power and platforms available?	Broadband/mobile penetration

Example 3.1 — E-readiness gap analysis

A district office plans an online land-record service. Land records exist only as handwritten registers; there is no law recognising digital copies; staff have never used computers; the office has unreliable electricity. Identify the e-readiness gaps.

Solution

Data system: records not digitised → need scanning, data entry, verification.

Legal: no recognition of digital copies → need legal amendment / e-signature rules.

Human: staff untrained → need ICT training and change management.

Technological: unreliable power → need power backup, network and hardware.

Institutional: assign a responsible unit and re-engineer the record-updating procedure.

3.2 Evolutionary Stages in E-Governance

E-governance usually develops through stages. Different authors propose different numbers, but the common idea is that an agency moves from simply *being on the web* to *transforming the way it governs*. A commonly cited sequence is:

Stage	What happens	Example
1. Emerging / Presence	Government websites provide basic, static information.	Ministry site with contacts and notices.
2. Enhanced / Interaction	Downloadable forms, e-mail contact, search, simple feedback.	Download application form; send query by e-mail.
3. Transactional	Full online services with payments and authentication.	Online tax filing and bill payment.
4. Connected / Integrated	Back-office integration, data sharing, single window.	One portal for several departments' services.
5. Transformed / Seamless	Citizen-centred, proactive, personalised services; participation.	Services delivered automatically on life events.

Another well-known view (the Layne & Lee model) describes stages as **cataloguing → transaction → vertical integration → horizontal integration**. Vertical integration links different levels of government for the same function (federal–provincial–local); horizontal integration links different functions or departments at the same level.

Note: Treat stage names as flexible; examiners usually expect you to explain the progression and give an example for each stage.

3.3 Strategies for Success

Many e-governance projects fail — they are over budget, abandoned or not used. Research on such failures points to a mismatch between *design* and *reality* (the “design–reality gap”). The following strategies improve the chance of success.

Strategy	Explanation
Clear vision and master plan	Define goals, priorities, phases and measurable outcomes; align with national development plans.
Leadership and political will	Strong sponsorship from top leaders; a project champion.
Citizen-centred design	Understand user needs; involve users from the start; simple, local-language, accessible services.
Business-process re-engineering	Simplify and redesign procedures first — do not just computerise a bad process.
Phased implementation and pilots	Start with high-impact, achievable projects; scale up after learning.
Capacity building	Train staff and citizens; manage change; create incentives.
Standards and interoperability	Common standards, architecture and shared platforms to avoid silos.
Legal and policy support	Enabling laws, privacy and security rules.
Security and trust	Authentication, encryption, audits and privacy safeguards.
Partnerships (PPP)	Use private sector and civil-society skills and funds where appropriate.
Monitoring and evaluation	Indicators, feedback, audits; improve continuously.
Sustainability	Funding for operation and maintenance, ownership by the department, exit strategy for donors.

Typical Reasons for Failure

- Total failure — project never implemented or abandoned immediately.
- Partial failure — major goals not achieved or undesirable results.
- Sustainability failure — works at first but collapses after funding or champion leaves.

Example 3.2 — Exam question

List and briefly explain five strategies that can make an e-governance project successful.

Solution (outline)

(1) **Clear vision and plan** – goals, phases and indicators. (2) **Leadership** – top-level commitment. (3) **Process re-engineering** – simplify before automating. (4) **Capacity building** – train staff and citizens. (5) **Citizen-centred, secure and interoperable design** – user involvement, standards and security. Add monitoring and sustainability if marks allow.

Key Takeaways — Unit 3

- ✓ E-readiness = preparedness of data, legal, institutional, human and technological infrastructure.
- ✓ Data must be digital, standardised and shareable; laws must recognise electronic transactions.
- ✓ Institutions and leadership coordinate; people need skills and willingness; technology provides the physical base.
- ✓ Stages move from presence → interaction → transaction → integration → transformation.
- ✓ Success needs vision, leadership, BPR, capacity building, standards, security, phased delivery and sustainability.

— *End of Unit 3* —

Reminder: these notes may contain errors — verify with your textbook and class notes.

bcalink.com