Annex 5: Application Architecture, Regulatory framework and e-readiness issues in the eModel

1. Application Architecture

e-Government application projects are strongly influenced by existing data, systems and processes, which constitute a legacy that in many cases requires a “rethink”, rebuilding and renovation of the underlying data system and application architecture. Moreover, e-Government programs need stronger and more flexible support to be provided by applications to improve the efficiency/effectiveness of government administration, deliver services through different channels and integrate the back office processes in a comprehensive way.

This E-Model provides a set of guidelines to be followed in order to identify the target architecture for a country that wishes to start an e-Government program, a guide to the common risks that countries normally face during the implementation phase, and a (by no means exhaustive) collection of good practice references for e-Government solutions.

The guidelines are based directly on the guiding principles that identify “best practice in government administration” and on the general legacy constraints of implementing countries.

1.1 Application architecture requirements

The application architecture requirements follow on directly from the main requirements for e-Government as outlined above (see Figure 1).

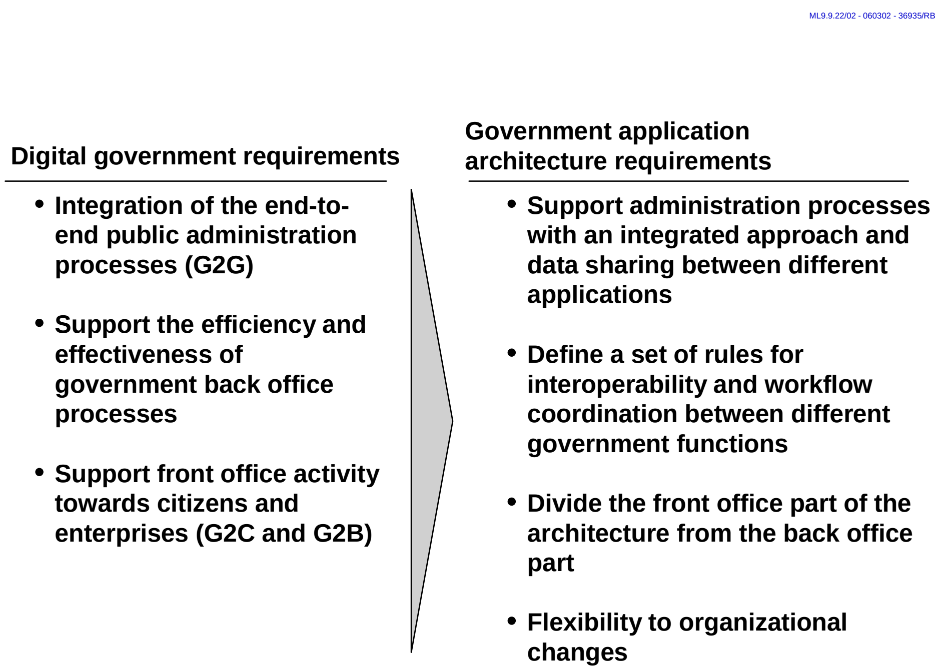


Figure 1: Government application architecture requirements

These government requirements can be translated into a set of architecture requirements that must be complied with. In particular, a good practice government application architecture must be able to:

- Support both specific government functions (through “vertical” applications) and shared government functions (through “horizontal” applications) and adopt an integrated approach to this process. To do this, it is necessary to define a set of general rules that can drive both the integration between "horizontal" and "vertical" applications, and data sharing between different applications.

- Deliver services with an end-to-end approach to processes, integrating all the government functions involved in them. To satisfy this requirement it is necessary to define a set of rules for interoperability and workflow coordination between different government functions.
- Allow a multi-channel strategy. The target architecture must be designed taking a multi-channel approach (even if the multi-channel distribution is not immediately implemented), separating the front office part of the architecture from the back office part.
- Respond flexibly to organizational changes. To do this it is necessary to subdivide processes into elementary and consistent steps that can easily be assigned to different organizational functions.

Legacy constraint problems must be evaluated case by case; clearly, they are more relevant in cases where the government has been investing in ICT for several years.

1.2 Interoperability

The overall integration and harmonization of public transactions and data is particularly relevant to the processes that must be established to manage the data flow and exchange of services among different agencies, both for back and front office activities.

The adoption of a common general model to ensure cooperation between architectural applications enables a smooth interaction between citizens and the various agencies, independently of the specific platforms and solutions adopted by each agency.

In this way citizens who needs to interact concurrently with several agencies can rely on a single seamless interface that will allow them to navigate through different services, provided by different sources, with as little inconvenience as possible. Similarly, when two different agencies need to interact to establish common back office procedures, the presence of a standard exchange interface ensures that the data and service flows are set up correctly.

The presence of a common, standard exchange interface ensures technological heterogeneity, which is intrinsic to the growing "pathway" of ICT infrastructures within each agency, and ensures that local technical solutions are independent. This kind of plug-in communication interface is shown in Figure 2.

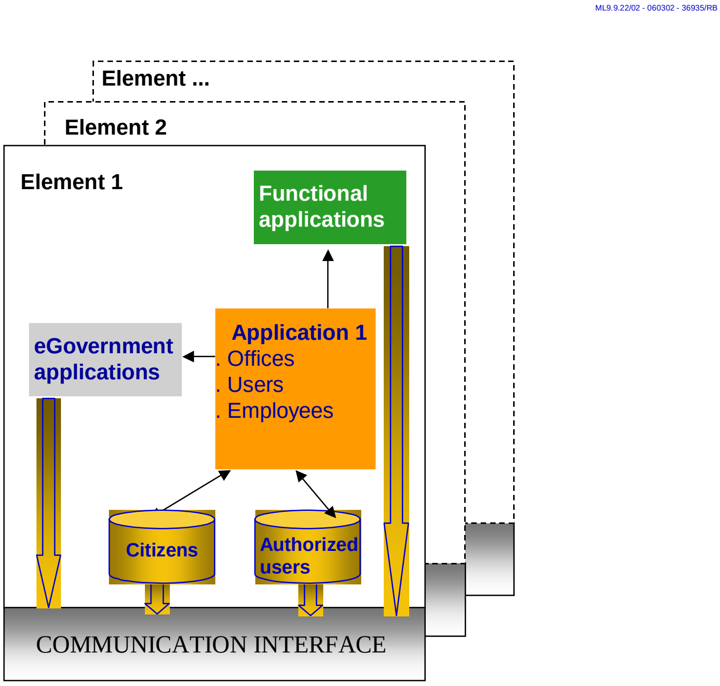


Figure 2: Plug –in communication interface.

Through the adoption of a common exchange interface that acts as a standard plug-in for any application, a common cooperative process is established to automatically exchange information and services between ICT applications, complying with all the requirements of:

- Authorization
- Identification
- Integrity and privacy

This solution provides, without any impact on any information system that may already be in place, the maximum degree of integration between agencies. The deployment of such a solution only requires the definition and agreement of some common communication services and the way in which they are to be interchanged.

The creation of a cooperative process between the ICT applications of different agencies covers several needs:

- Events communication: one agency automatically notifies to one or more other agencies the occurrence of a life event of a citizen or enterprise
- Queries: requests for access or notification to one or more agencies of data managed by one or more other agencies
- Transactions between agencies: transactional services, which modify the content of the information managed in the local info-base of another agency.

1.3 Implementation guidelines

This section provides a set of recommendations that can help interested countries in validating their implementation options.

Addressing integration issues

- Share across-government functions and the development of applications that support common administrative processes (for example, procurement, document management, human resource management. See also Exhibit 6).
- Integrate the application across the end-to-end processes by defining a standard set of rules for interoperability.
  - Each application must interact with the others through clearly identified interfaces.
  - Data common to several processes must be collected and managed as a shared resource (one single logical database).
  - Process steps, rules and actors must be modeled and automated through workflow, particularly when process changes are frequent and there is a strong need for tracking controls. To achieve these objectives, it is necessary to distinguish processes that are common to more than one function (horizontal processes) from those that are function-specific (vertical processes) to eliminate any overlap of software layers and reduce data redundancy.
  - Data exchanges between functions must be certified and tracked in order to manage the responsibility clearly.
- Enhance the portability of services to a multi-channel distribution model. To do this it is necessary to completely separate the front office side of service provisioning from the back office operations. Using this approach, a service can have the same back office process and application and a different front office process and application for each distribution channel, thus simplifying the portability of the service over different channels.

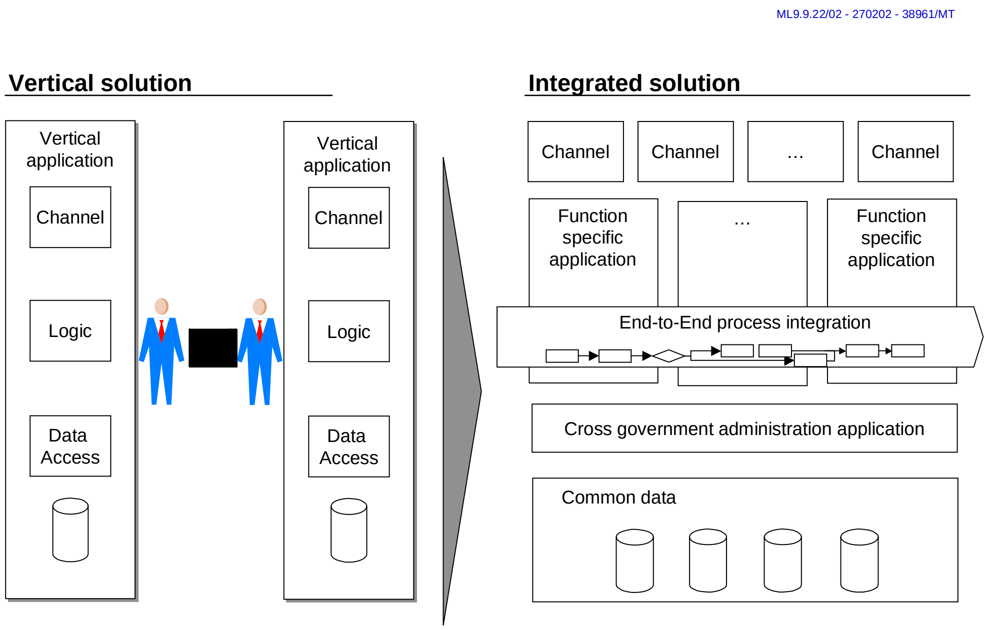


Figure 4: From vertical solutions to integration

1.4 Common data management

Data management must be considered critical when moving to e-Government. The government of any country owns significant information assets, in terms of documents and electronic data, which cover all citizens' and enterprises' significant life events (economic, social, local and so on).

These data, named common data, are those critical pieces of information that must be accessible if citizens and enterprises are to exercise their rights and fulfill their obligations. Common data can also be defined as the complete set of data, owned by the government, which have been collected and/or processed, within the administrations' institutional competencies, using public funds.

The stakeholders in this process are the public agencies, who "own" and must make available the data, the private actors in question (any individual or enterprise) and the community as a whole.

The set of rules that need to be applied to make the public data available to all the subjects involved are described using the term "*common data availability*".

Common data can be made available in three different ways.

- Access: the process is started by the user, who can search for the required data and gain access directly over the network; it is worth noting that here by "user" we mean either a person or an automated application which is part of an information system;
- Communication: the process is started by a public agency or by a user, who makes a request, and consists of delivering data to one or more recipients by electronic means;
- Dissemination: this is an initiative by the government, through which data are made available to a large audience, not determined in advance, using the Internet or more traditional media.

Public agencies, which are entrusted with the process of gathering, processing and publishing common data, must set the rules for the following fundamental aspects: classification, availability, security and usability.

Classification

For those issues relevant to data classification it is necessary to:

- select, from all public data, those which should be considered essential;
- enact regulations (legislative) to ensure their availability;
- issue technical regulations to prevent, or make as difficult as possible, the building of new files, based on the essential public data, that might violate the privacy of citizens or enterprises. Specifically, this measure must play a part in enhancing the level of privacy using whichever means are feasible;
- set out rules to ensure that access to sensitive data is only allowed when strict procedures are complied with.

Table 3 shows the significant characteristics that must be taken into account when classifying common data.

Table 3: Data classification parameters

Type	*personal or anonymous*
Source	*delivering agency, date*
Level of aggregation	*with which the aspects of reality to be investigated are described*

Usefulness	*for those users who intend to access it*
Level of elaboration	*from raw data to final indicators*

Availability

With reference to common data availability, it is important to ensure that the following conditions are in place:

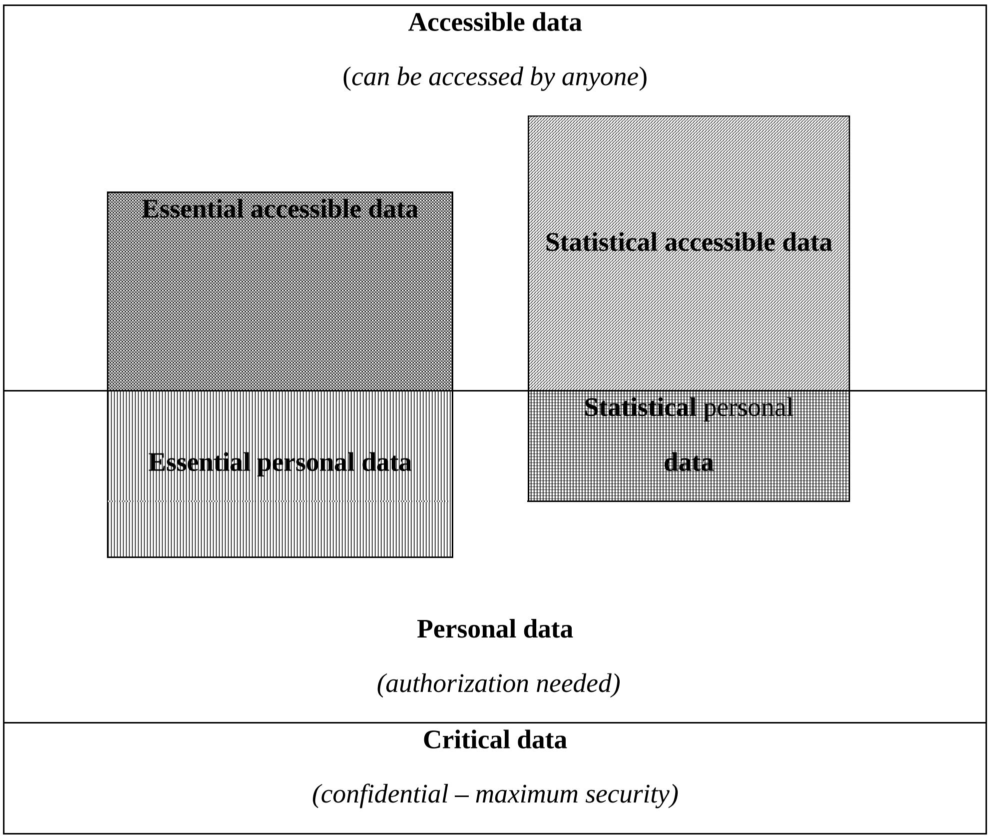
- the ability of the public owners to inform users about the availability of public data and clearly explain how to reach them (through access, communication or dissemination) according to the nature of the data and the user authorization level;
- data availability by means that do not cause disadvantages to any particular category of users compared with other categories;
- the definition of models for public data availability, such as:
  - ability of the owner (citizen or enterprise) to access, verify and, if needed, update directly his or her personal data or the business data;
  - search facilitation and access, by all members of the public, to anonymous data;
- the definition of access policies, organizational rules for publicly accessible data repositories and their relative service levels vis-à-vis end users;
- the adoption of technical and organizational solutions to offer users quick and high quality assistance;
- adequate dissemination of the conditions (e.g. responsibilities, timescale, service levels, assistance, security etc) under which non-essential data are made available, along with their quality characteristics.

Security

The issue of common data security (see Table 1) addresses all those aspects that are common to public and private data distributors, in relation to:

- the adoption of internal security measures to ensure the availability, confidentiality and integrity of public data;
- the formulation of external security measures that final users (i.e. citizens and businesses) are required to comply with if they wish to access public data;
- the identification of the person(s), in terms of role(s) inside the government, with responsibility for the security of public data.

Table 1: Data access levels



Usability

Finally**,** usability as used here means ease and simplicity of access by any authorized user, through the enabling platforms made available by the latest technologies. Here again, the approach must be a non-discriminatory one that takes into account any possible obstacle to the access and dissemination policies. Usability is measured, in terms of effort required from the user, by:

- ease of learning, for users to gain the ability to use the technologies necessary to access the data;
- understandability, for users to understand how the technologies work;
- operability, for users to actually make use of the technologies to access the data they are interested in.

In an inter-networked information system, quality aspects of common data are crucial; these aspects must ensure for all exchanged data:

- correctness: the data must correspond exactly to the observed information;
- timeliness: when the phenomenon they represent changes, data must be updated fast enough for the update to be effective for subsequent use of the data ;
- consistency: between the different representations which can co-exist in networked systems;
- non-redundancy: to minimize the number of different occurrences of data describing the same phenomenon in different, interacting information systems;
- accuracy: measurability of the precision of the data.
- pertinent and non-superfluous information: in relation to the use that will be made of the data.

Only if all the above-mentioned quality aspects are complied with the establishment of reliable, optimized and easily manageable dataflow can be ensured, both between agencies and towards final users (citizens and enterprises).

When designing or re-engineering an information system or part of one, it is essential to avoid, or at least to keep to a minimum, data redundancy and duplication, since these generate an unproductive workload, in terms of to managing data mismatches and assessing original sources.

Therefore, it is strongly recommended that rules and obligations be clearly defined, with the appropriate level of detail, for each agency, in terms of access, management and protection and dissemination of public data.

With reference more specifically to back-office processes, responsibilities must take into account the questions of *ownership* and *authorized access levels* (i.e. browse, update, delete, manage) for data processed by applications shared between different agencies.

It will therefore be necessary to set common rules to**:**

- define representation standards for the information exchanged between agencies;
- enable each agency to determine the different types of data and information that are to be made available;
- draw up, with the involvement of all the agencies concerned, a map of all data of common interest owned by an agency.

Given the strong need, as mentioned above, for data of common interest to be unique and non-redundant, once these maps are complete and data representation is determined and agreed, the next step in the model is to build common information bases for this kind of data, where the pieces of information are stored just once in a standard representation format.

All the applications from several different agencies will share this single common data repository, which will be made accessible with the appropriate level of authorization; a typical example is the public register for citizens and enterprises. In this way the quality requirements can be met with the minimum investment and operational effort.

2. Regulatory framework issues

The rules and regulations necessary for e-Government programs differ greatly from country to country, depending on the current social, constitutional and regulatory situation in the implementing country.

It is therefore necessary to define only the guiding principles that the regulatory system needs to follow. In fact, regulatory reform is one of the critical issues that has often been overlooked. Yet, experience has shown that it is crucial for e-Government success, both in terms of affordability and long-term sustainability. Regulatory reform is a “must do” to guide most e-Government applications. In cases where these applications were developed outside the appropriate regulatory framework, the chances of their completion are greatly reduced.

e-Government requires the establishment of a range of suitable legal and regulatory measures that are aimed at:

- Integrating and sharing data systems within and among administrations
- The use of this public information by third parties, especially the private sector, safeguarding privacy and security issues
- Enabling the digital exchange of information and transactions between government agencies, citizens and businesses.
- Recognizing the digital exchange of information and allowing electronic transactions and record keeping
- Reaching citizens affordably and enabling citizens to reach government affordably by facilitating availability of and access to information and communication services

Throughout the world concerns are being raised about the safety of electronic information transfer and storage. Governments must ensure that e-Government is preceded by changes in the legal system to protect information and privacy in the digital age. At the same time criminal codes need to be upgraded to incorporate cyber-crime and the stealing of electronic data. The legislation governing intellectual property rights must be amended to include the protection of e-content ownership.

One of the most significant issues from the legislative point of view is therefore the regulation of public data distributors, with regard to:

- an indication of the types of public data that can be made known and, of these, the types considered as essential and the public actors distributing them;
- indication of rating criteria for data declared suitable for the public domain;
- indication of the principles on the basis of which to define licensing systems for the (re)-diffusion of public data;
- public tenders for the (re)-diffusion of public data by private operators;
- legal validity of digital representation of data with respect to traditional means of representation, by both public and private distributors.

To ensure data quality the following will be indispensable:

- issuing of quality standards for public data;
- ban on acquisition of data already held by the public body concerned (possibly in terms of general profile), by reversing the transmission cycle;
- indication of the timescale for the up-dating of public data declared suitable for the public domain with respect to the timescale involved in collecting the data.

Countries should be ready to adapt their legislative framework to apply "electronic equivalents" of traditional paper procedures, such as personal identification, signing and filing. Legislation should therefore identify types and standards for electronic signatures and authentication and allow and regulate electronic record keeping.

In addition, the move towards more intra- and inter-government information sharing, required by e-Government, necessitates legislation that validates and regulates access to such information and to data matching.

Accessibility to government by citizens and to citizens by government can be facilitated by legal solutions that can affect the availability and accessibility of telecommunication services, such as the liberalization of the telecommunication market, the establishment of independent regulators and pro-competitive regulation measures and the introduction of fiscal benefits for investment in telecommunication infrastructure and in hardware and software, mainly through a review of domestic and import taxation on ICT related equipment, parts and software.

Other reforms may prove to be necessary in order to regulate the internal organization of government, with the objective of facilitating the adoption of e-Government. In particular, the process of streamlining administrative procedures could eliminate barriers to its deployment.

3. E-Readiness issues

The objective of this phase is to support the preparation of a pre-feasibility assessment.

Before defining an e-Government for development strategy or plan of action, a thorough analysis is required of the existing environment in which e-Government will be implemented. Government can pose itself some key questions in order to assess how strategically prepared it is for e-Government.

A country level of "e-Government readiness" is the degree to which each country is prepared for the introduction of e-Government. By assessing the relative state of advancement in the areas that are most critical for the adoption of e-Government for different key factors, countries will be in a better position to evaluate opportunities and challenges, as well as their own strengths and weaknesses.

However, as uniformity across the broad is impossible, the objective of the e-readiness analysis is to identify specific actions for improvements and potential niches for the initial start up of e-Government programs, rather than a positive or negative answer to e-Government as a whole.

Focusing on the readiness assessment for e-Government, the following areas and key factors (see Table 2) should be carefully analyzed in order to examine the risks and assess the obstacles that may need to be overcome before entering into e-Government.[1]

Table 2: E-Readiness factors

Areas	***Key Factors***
Political conditions Good governance, as a condition for sustainable development, requires genuine commitment from political leaders, the private sector and organizations of civil society. In the same way, the introduction of e-Government in society requires a strong political will to see through the transformation process it implies for government both in its internal operations and with regard to its interaction with civil society.	• • Awareness of political value of e-Government • Commitment to e-Government and good governance • Leadership skills • National identity and perception of government • Legislative framework • Citizens' and civil society's participation in government's affairs • Good governance and rule of law
Regulatory framework A proper regulatory framework is needed in order to enable secure information exchanges within government and between government, citizens and businesses. It is also needed to create the economic conditions for accessible ICT infrastructures, services, and equipment	• • Security standards • Privacy legislation • Legal validity of online transactions • Degree of liberalization of telecommunication market, including the internet service providers market • Positive fiscal environment for acquisition of IT equipment
Organizational conditions International experience shows that the introduction of e-Government calls for and causes profound and evolutionary change in the institutional arrangements. To guide this transformation process, appropriate management and coordination mechanisms are needed.	• Administrative structures and legacies • Public administration reforms • Civil service reform • Central coordination and support unit • Policy coordination • Inter-governmental relations • Change agents and management
Cultural and human resources conditions	

[1] In the past years several institutions have developed specific methodologies – e-readiness tools – that may assist developing countries in assessing their status of readiness to participate in the networked world and to share in the benefits of the Internet. For a presentation of the main e-readiness tools and selection criteria see the InfoDev e-readiness section at http://www.infodev.org/ereadiness/. Some major institutions are in the process of developing readiness tools for e-Government specifically targeted to developing countries. The subsequent versions of the Reference Model will include references to these tools as soon as they are made available to the public.

Positive attitudes, knowledge and skills need to be in place – especially within the public sector – to initiate, implement and sustain e-Government. Cultural aspects may cause general resistance to change and information-sharing. Inadequate human resource capacity may lead to lack of customer-orientation and overall commitment.	• Culture, traditions and languages • Gender inequality • Educational levels • IT literacy and number of online users • IT educational facilities and programs • Culture of information and knowledge sharing • Prevailing organizational culture • Attitude and adaptability to change, especially in public administration • Managerial skills in the public sector • Service orientation of public administration towards citizens
Financial conditions and sustainability of the projects	
The initial costs related to implementing e-Government can be considerable and Governments may have limited capacity to bridge the period between initial investments and returns. Proper resource planning and access to innovative funding mechanisms is critical for e-Government sustainability.	• Resource allocation process • National income structure • Access to alternative financing mechanisms • Partnerships with private sector and other players • Access to capital markets • Mechanisms for venture investment • Available financial resources
Communication environment	
In today's world, communicating with citizens is a duty and a necessity for governments. E-Government needs to be accepted and understood by all stakeholders to ensure that its benefits flow to society as a whole.	• Citizens' awareness and understanding of ICT and e-Government • Communication culture and channels • Information and knowledge sharing
Technological Infrastructure	
Lack of technologies is a major bottleneck for countries aiming to implement and maintain e-Government. Legacy systems may also represent considerable obstacles to change. The demographic and geographic conditions of different areas, accompanied by the distribution of economic activities, may also represent a strong bias in the rollout of ICT infrastructure if left to the market alone.	• (Tele) communications infrastructure • Penetration rates of telecommunications • Urban versus rural: demographic/geographic bias • Software and hardware (legacy systems) • IT standards
Data and information systems	
Management systems, records and work processes must be in place to provide the necessary data to support the move to e-Government.	• Legacy of data processing, management information and decision support systems • Available and accessible data and information • Data collection procedures and data and information standardization • Data and information quality and data security • Capacity to analyze data and utilize information • Capacity to direct information flows into decision-making processes • Information policy

Countries should update this environmental analysis on a regular basis to reassess their readiness against technological progress and on-going changes in the governance system.