Info-Structure: e-Records

1. Infra- and Info-Structure for e-Government

An imperative task in e-government development is the establishment of Government Information Infrastructure (GII), which aligns a government’s existing communications infrastructure with the implementation of a Government-wide Data Network (GDN). There is no doubt that an integrated architecture model for government infrastructure is critical for the support of electronic service delivery and government operations. In order to enhance service delivery, a framework and a platform are needed to enable interoperability among government programmes, both for information sharing and for business transactions.

However, e-government cannot be implemented through data communications infrastructure alone. Establishing trust and confidence in electronic transactions is also a must in order to assure people that their privacy is protected and their transactions are secure. For this purpose, security mechanisms, such as authentication and digital signatures, must be put in place along with the implementation of GII. As far as the digitization of information is concerned, a common infrastructure related to information content in areas such as electronic records and portals is also an emerging priority and has become increasingly significant. In addition, electronic payment is an indispensable means for online transactions. Information-related infrastructure that is fundamental to the implementation of e-government is called ‘info-structure’. In subsequent modules a number of important info-structures will be introduced. Actually, many governments have been working towards a common info-infrastructure to pave the way for e-government development.

2. What is an e-Record?

Records play a vital role in the process of government activities. They provide an historical record of decisions, changes, and outcomes. The introduction of the computer has made an enormous impact on the way that information is created, transferred, and stored.

A record is defined as ‘a unit of information in a computer database identifying a specific item. It includes data such as author, title, date, publisher, subject headings.’ Records play a significant role in providing evidence to support the rule of law, and in supporting the accountability of government administration.

With the emergence of information technology in daily operational activities, an increasing number of electronic records are being created, either by being converted into digital form or by being ‘born’ electronically. Electronic records include numeric, graphic, and text information, which may be recorded on any medium capable of being read by a computer and which satisfies the definition of a record. This includes, but is not limited to, magnetic media, such as tapes and disks, and optical disks. Electronic records may exist in all electronic information systems, whether on microcomputers, minicomputers, servers, or mainframe computers, regardless of storage media, in network or stand-alone

1 'Keeping Electronic Records Forever' by The Public Record Office of Victoria, Australia; 'Managing electronic Records' by National archives of Australia; and 'The Preservation Management of Digital Material Handbook' by the Digital Preservation Coalition are the main references for this session.
configurations. Electronic records may also be any combination of text, graphics, data, audio, pictorial, or other information presented in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system. Records are evidence of business transactions captured electronically and examples include Microsoft Word documents; e-mail messages; Microsoft Excel worksheets, etc.

Furthermore, electronic records may be based on transfers, which occur within and between computer systems. These records may be updated, deleted, altered or manipulated without human intervention. The essential characteristic of the record content, structure, and context may be altered or lost during this process. Therefore, records are no longer defined in terms of the physical objects which carry them. A record can be ‘carried’ or created in various media and formats.

When electronic documents are required to be kept as a record to meet legal requirements or in the ongoing conduct of business, they must have the following properties:

- They are created digitally using a variety of word processing, database, and graphics packages.
- They can be rendered differently on screen and through a variety of printers, plotters, or fax.
- They may be stored locally, copied, distributed and modified by multiple authors, before becoming a record. They may continue to be modified and re-used after meeting the criteria of record status.

3. Benefit from Managing e-Records

E-records permeate our everyday life and have the following benefits.

When e-records are managed effectively, they support online business. A record of an online transaction can be captured which is a requirement for all kinds of online business. Such transactions and decisions, or the information behind those transactions and decisions, may never appear in paper form. These records are created electronically and remain in an electronic format for their entire life; they provide the evidence of those transactions.

The volume of e-records often makes paper records unworkable. For example, large amounts of information can be recorded on a CD-ROM. As a result of the exponential growth in the electronic data and information environment, e-records have many advantages over paper-based or microform records in terms of convenience and functionality. E-records provide many ways to get information, link people to people, and information to history. In addition, e-records create significant and continual reductions in the cost of record storage. This may reduce the storage of paper records and help avoid cost escalations.

E-records can be accessed at any time, and employees and citizens can access them through the Internet. The increasing proliferation of digital information and the need to ensure continued access to it has important implications for libraries and archives. It can help to facilitate the transfer of records between agencies and departments, and to provide a rich framework of metadata to aid access.

There is public concern over government accountability. An effectively managed e-record and archive system identifies a government as a proactive and innovative leader in the IT revolution. E-records provide a ‘picture’ of our society and culture and the issues and environment in which they exist. There is a growing expectation of online access to public records available to the general public.
Governments are relying more than ever on an effective and reliable e-records management, including the creation, transfer, and storage process.

4. Challenges with e-Records

The dependence of e-record on hardware and software, combined with rapid cycles of technological obsolescence, makes an e-record inherently fragile. All organizations are facing a dilemma of the consistent and reliable migration of records between all applications currently in use and those yet to be developed. To date, most e-records and the computer application in which they were created are inseparable. In order to access and give future meaning to e-records created today, it is necessary to migrate the application with which the record was created. As the number of e-records increase, so does the challenge of access.

It is obvious that in the case of e-records, concentrating on preserving the physical carriers will not suffice. The computer systems must be specifically designed with a record-keeping functionality to ensure that the essential characteristics of the records will be maintained. Moreover, although the carriers, such as tapes, CD-ROMs, etc., may last for relatively lengthy periods of time, the records they carry may effectively cease to exist because the technology necessary to retrieve them is no longer available or supported by the manufacturer. On the other hand, the storage media are inherently unstable, and without suitable storage conditions and management, they can deteriorate very quickly even though they may not appear to be damaged externally.

The greatest threats to e-records are obsolescence of the storage technology and failure of the storage media. The occurrence of either could prove disastrous to maintaining e-records for long periods of time. However, there are other challenges associated with maintaining a secure, reliable, and trustworthy e-record system.

Any e-record system should perform in an accurate, reliable, and consistent manner, so that e-records are always accurate and available for retrieval. A government will be increasingly vulnerable to future legal action without an effective and reliable e-record system. Governments are increasingly making decisions based on information provided in an electronic format, for example, e-mail, or spreadsheet, the contents of databases or word-processed documents received in an electronic form, all of which could form parts of records that are never printed or signed. These types of records are challenging today’s record management system and are creating problems that need to be solved.

E-records can be altered or deleted, either consciously or inadvertently, and their inviolability for evidentiary reasons is difficult to ensure. Currently, it is possible to change an e-record and leave no trace of the change. Standards for a controlled e-record storage system to ensure an e-record’s integrity and accessibility should be maintained.

Finally, there is the challenge of access to authentic copies in usable formats for legal retention periods. The mechanism for both e-record authenticity and user authenticity should be taken into consideration when the e-record system is being designed and implemented.

The issues discussed above are all interconnected. They indicate that a radically different approach is required in managing an e-record system to a paper-based one. It is imperative to solve the issues of capturing, storing, accessing, and recreating e-records. Action needs to be taken as early as possible; plans should be updated at regular intervals, and throughout the lifecycle of record management. In addition, a comprehensive organizational change management strategy should be developed and implemented to minimize the risk associated with personnel and cultural issues and to facilitate the introduction of new technologies and processes into operational environments.
5. Technologies in Use

Preservation of the static content of an e-record is critical. Systems must ensure that the content is viewable in the future by technologies that are not available today. While media upgrades leave data unchanged, the data must be transferred, so that system upgrades do not leave behind legacy data. Meanwhile upgrades to the print, index and search systems should not affect the content of an e-record. The preservation of an electronic document means the ability to reproduce on paper or on a screen the same approximate form of the same content at any time in the future.

Currently, there are several kinds of output formats which support the key properties of an e-record. Those formats include:

- **Tiff.** An image oriented interchange format using pixel-oriented techniques.
- **Postscript.** A common language used to describe page layouts for printers.
- **PDF.** A language specifically designed for recording the form (or rendering) of electronic documents.
- **SGML.** The best representative of formats related to recording the structure and content of information.

These formats are more or less useful depending on the type of e-record under consideration – word processing, email, database or computer aided design. Some observations about this follow.

5.1 Word Processing Document

In word processing documents format:

- Tiff can capture the form of a document but it is not well integrated into applications and does not directly support indexing and compactness requirements.
- Postscript has high levels of application support, and it supports some word extraction for indexing but has low compactness.
- In terms of indexing support and compactness, PDF is an advance on Postscript, but it is a recent addition and has little application support. Additional tools can be used to convert Postscript into PDF.
- SGML supports very high levels of indexing and compactness but is unable to support the generation of the original form, because the application to this sort of record of information is outside of the normal function of SGML.

5.2 E-Mail

E-mail is a major problem with reference to e-record-keeping. A well-defined strategy is needed to incorporate e-mail information into record management systems. E-mail replaces paper-based communications and merges the properties of fax and voice communications. As a result, it can be treated in court as formal and evidential. The text with appropriate header information might be sufficient for the storage of current e-mail messages. However, there is a trend to include HTML formatting capabilities that might prove useful.
5.3 Database

Electronic databases are an official record of the current state, as well as the results of decision-making. The contents of databases can be preserved by developing SGML encodings (DTDs) suitable for their contents and by periodically dumping the database into this format for storage. The structured format, along with the metadata required to access the data and their links, can be defined in the way they were originally recorded and preserved.

5.4 Computer Aided Design Documents

GIS and CAD systems are increasingly becoming part of electronic documents. To form part of an e-record, a viewing system needs to be developed and maintained. There are standards covering the developing requirement for capturing 3-D diagrams. 3-D models are similar to multimedia and an understanding of how to capture 3-D diagrams as records can help to further the understanding of how to do the same for multimedia.

New elements and versions of technology constantly appear, driven by the imperative of global business for the distribution of non-proprietary electronic document processing. The production of these new elements and versions is supported through

- The exponential development and growth of the Internet, Web and Intranet systems and the corresponding technologies and standards for the interlocking of distributed authoring and viewing systems.
- Standardization in the formats of printing systems and their interface applications.
- Standardization in transaction formats with the ongoing development of e-commerce, e-government, and EDI.
- Standardization in the nature of document components and methods used to support embedded document components, through the development of object linking and OpenDoc architectures and systems.
- The technology of CORBA and other distributed object-based software systems, especially Java, which allows remote access to application code required by document components.
- The density development and standardization of multimedia consumer products that is suitable for domestic long-term mass storage and information handling and dissemination.

6. E-Record Management

E-record management includes the planning, controlling, directing, organizing, training, promoting, and other managerial activities involved in the creation, maintenance and use, and disposition of e-records. The aim is to achieve adequate and proper documentation of the policies and transactions of the government, and effective and economical management of agency operations. An organization’s e-records management process should cover their entire life cycle of the record, from creation and maintenance, to adequate documentation and proper disposition.

Government agencies need to develop and maintain up-to-date documentation about all electronic information systems. Documentation that is able to adequately specify all technical characteristics necessary for reading or processing the e-records; identify all defined inputs and outputs of the system;
define the contents of the files and e-records; determine restrictions on access and use; and understand the purpose(s) and function(s) of the system. The documentation must also be able to describe update cycles or conditions and rules for adding information to the system, and for changing or deleting information in it. It must also ensure the timely, authorized disposition of records. Government agencies should specify the location, manner, and media in which e-records must be maintained in order to meet operational and archival requirements. They must also maintain inventories of electronic information systems to facilitate disposition.

Each government agency should assign to one or more offices of the agency the responsibility for the development and implementation of agency-wide programmes to identify, develop, issue, and periodically review e-record-keeping requirements for all agency activities, at all levels and locations, and in all media. This will include digitizing traditional media, such as paper, microform, audiovisual, cartographic, etc. and electronic media including those created or received using electronic mail. Each government agency should integrate its programmes for the identification, development, issuance, and periodic review of e-record-keeping requirements with its other programmes for the management of records and information resources.

Adequate training should be provided to all agency personnel on policies, responsibilities, and techniques for the implementation of e-record-keeping requirements. The training should include definitions of e-records and should explore and explain the difference between material that is an e-record and that which is not regardless of particular media and including those materials created by individuals using computers to send or receive electronic mail.

6.1 Creation of e-Records

The statutory definition of government e-records should be defined and documented by the appropriate government authorities, and key terms, phrases, and concepts in the statutory definition of e-records should also be clearly defined.

In general, adequate management controls over the creation of government agency e-records should be instituted to ensure that agency functions are adequately and properly documented. In this regard, government regulations on creation of e-records should be established as well.

Government e-record-keeping systems that maintain the official file copies of text documents on electronic media should meet the following minimum requirements:

1. Provide a method for all authorized users of the system to retrieve documents, such as an indexing or text search system.

2. Provide an appropriate level of security to ensure the integrity of documents.

3. Provide a standard interchange format when necessary to permit the exchange of documents on electronic media between agency computers using different software/operating systems and the conversion or migration of documents on electronic media from one system to another.

4. Provide for the disposition of documents, including, when necessary, the requirements for transferring permanent records to government archives authorities.

Before a document is created electronically on an electronic record-keeping system, which will maintain the official file copies on electronic media, each document should be identified sufficiently to enable authorized personnel to retrieve, protect, and carry out the disposition of documents in the system. Appropriate identifying information for each document maintained on the electronic media may
include: office of origin, file code, key words for retrieval, addressee (if any), signatory, author, date, authorized disposition (coded or otherwise), and security classification (if applicable). Agencies should ensure that records maintained in such systems can be correlated with related records on paper, microform, or other media.

6.2 Maintenance and Use of e-Records

Government agencies must institute adequate e-records management controls over the maintenance and use of e-records wherever they are located to ensure that all e-records, regardless of format or medium, are organized, classified, and described to promote their accessibility, and to make them available for use by all appropriate agency staff for their authorized retention period. Agencies should also maintain permanent e-records in a format that will permit transfer to appropriate government archives authorities.

Agencies should prescribe an appropriate e-records maintenance programme so that complete e-records are filed or otherwise identified and preserved; e-records can be found when needed; the identification and retention of permanent e-records are facilitated; and permanent and temporary e-records are physically segregated.

Government agencies should ensure that they maintain adequate information about their e-records moved to an off-site e-records storage facility. Agencies must also create and maintain e-records that document the destruction of temporary e-records and the transfer of permanent e-records to appropriate government archives authorities. The disposition of e-records that provide such documentation should be governed by corresponding government regulations.

Government agencies should select appropriate media and systems for storing agency records throughout their life, which meet the following requirements:

1. Permit easy retrieval in a timely fashion.
2. Facilitate distinction between record and non-record material.
3. Retain the records in a usable format until their authorized disposition date.

If the media contains permanent records and does not meet the requirements for transferring permanent records to government archives authorities, migration should be permitted of the permanent records at the time of transfer to a medium that does meet the requirements.

6.3 Retention and Disposition of e-Records

So that permanent e-records are preserved, Government agencies must ensure the proper, authorized disposition of their e-records, regardless of format or medium. They must also ensure that temporary e-records, no longer of use to an agency, are promptly deleted or disposed of in accordance with the approved e-records schedule when their required retention period expires. As an intermediate step, when e-records are not needed for current day-to-day reference, they may be transferred to an e-records storage facility.

For electronic information systems that produce, use, or store data files, disposition instructions for the data should be incorporated into the system’s design.

Agencies should establish policies and procedures to ensure that e-records and their documentation are retained as long as they are needed by the Government. These retention procedures should include provisions for
• Scheduling the disposition of all e-records, as well as related documentation and indexes. The information in electronic information systems, including those operated for a government by a contractor should be scheduled for disposition as soon as possible but no later than one year after the implementation of the system.

• Transferring a copy of the e-records and any related documentation and indexes to proper government archives authorities at the time specified in the records disposition schedule.

• Establishing procedures for regular recopying, reformatting, and other necessary maintenance to ensure the retention and usability of electronic records throughout their authorized life cycle. Electronic mail records should not be deleted or otherwise disposed of without prior disposition authority.

6.4 Security of e-Records

Government agencies should implement and maintain an effective records security programme that incorporates the following:

• Ensure that only authorized personnel have access to electronic records.

• Provide for backup and recovery of records to protect against information loss.

• Ensure that appropriate agency personnel are trained to safeguard sensitive or classified electronic records.

• Minimize the risk of unauthorized alteration or erasure of electronic records.

• Ensure that electronic records security is included in computer systems security plans prepared pursuant to relevant computer security acts.

6.5 Destruction of e-Records

E-records should be destroyed only in accordance with a records disposition schedule approved by the appropriate government archives authorities. Each government agency should ensure that:

• Electronic records scheduled for destruction are disposed of in a manner that ensures protection of any sensitive, proprietary, or national security information.

• Magnetic recording media previously used for e-records containing sensitive, proprietary, or national security information are not reused if the previously recorded information can be compromised through reuse.

• Agencies shall establish and implement procedures that specifically address the destruction of e-records generated by individuals employing electronic mail.

6.6 Management of Vital Records

Vital records include emergency plans and related records that specify how an agency is to respond to an emergency, as well as those records required to continue operations and protect legal and financial rights. Agencies should consider the informational content of records series and electronic records systems when identifying vital records. Only the most recent and complete source of the vital information needs to be treated as a vital record.

A government needs to prescribe policies and procedures for establishing a programme for the
identification and protection of vital records, including those records required by agencies for continuity of operations before, during, and after emergencies, and those records needed to protect the legal and financial rights of the government and persons affected by government activities. The records may be maintained on a variety of media. The management of vital records is part of an agency's continuity of its operational plan designed to meet emergency management responsibilities.

A vital records programme relates to the policies, plans, and procedures that have been developed and implemented. It covers the resources needed to identify, use, and protect the e-records essential for meeting operational responsibilities under national security emergencies or other conditions of emergency or disaster. It also covers e-records essential to the protection of the rights of the government or those of its citizens. This is a programme element of an agency's emergency management function.

Government agencies should ensure that retrieval procedures for vital records require only routine effort to locate the necessary information, especially since individuals unfamiliar with the records may need to use them during an emergency or disaster. Agencies also need to ensure that all the equipment needed to read vital records or copies of vital records will be available in case of emergency or disaster. In addition, for electronic records systems, agencies should ensure that system documentation, adequate to operate the system and access the records, will be available in case of emergency or disaster.

Agencies should take appropriate measures to ensure the survival of vital records or copies of vital records in case of emergency or disaster. In the case of electronic records, this requirement is met if the information needed in the event of emergency, or disaster, is available in a copy made for general security purposes, even when the copy contains other information.

6.7 Agency Internal Evaluation

Each government agency should periodically evaluate its e-records management programmes relating to the creation, keeping, maintenance, use and disposition of e-records. These evaluations shall include periodic monitoring of staff decisions about the e-record status of documentary materials in all media, and implementation of these decisions. These evaluations should determine compliance with the regulations established by appropriate government archives authorities, including requirements for the storage of agency e-records and the provision of e-records storage facilities. They should also assess the effectiveness of the agency's records management programme generally.
1. Introduction

In the physical world, it is easy to recognize who is who, either by seeing, by hearing, or by recognizing a person's handwriting. However, in the digital world, everybody is interfacing with each other on a computer screen. When organizations are moving their business transactions online, security and trust become critical requirements. Hence, authentication of identity, either of an individual or an organization, has become a primary issue. Digital signature, as a mechanism that speeds up transactions, saves costs, reduces paper, and improves transaction security, has been used widely as a fundamental component of business in cyberspace. A digital signature provides data integrity and proof of origin (non-repudiation). It can be kept by the receiver to settle disputes if the sender were to deny the content of the message or even to deny having sent it. Digital signature is also used for authentication to systems or applications.

2. What is Authentication?

The OSI Security Architecture (ISO7498-2) defines two kinds of authentication, entity authentication and data origin authentication.

1. Entity authentication verifies the identity of one entity by another. It is a connection-oriented operation. Entity authentication is typically achieved using an authentication exchange mechanism. Such a mechanism consists of an exchange of messages between a pair of entities, and is usually called an authentication protocol. Entity authentication includes unilateral authentication, which provides one entity with assurance of the other's identity but not vice versa, and mutual authentication, which provides both entities with assurance of each other's identity.

2. Data origin authentication provides corroboration to an entity that the source of received data is as claimed. However, the service does not, in itself, provide protection against duplication or modification of data units. Digital signature is a particular authentication technique that can be used to establish the origin of a message in order to settle disputes of what message (if any) was sent.

3. Basis of Authentication

In the networked world, it is not possible to authenticate a person in the same way as it is done in the physical world. Therefore, a basis for authentication is needed, which requires an authentication protocol to be built. Actually, the authentication is performed by an exchange of cryptographic messages – a shared secret between two entities. The so-called shared secret can be categorized into one the following three areas:

1. Something you know, a PIN or password. This is a knowledge-based authentication. In
this scenario, a person and the IT system share a pre-set PIN or password. A person is prompted to enter the PIN/password during authentication, and it is converted into a cryptographic key. This key is subsequently used in the authentication protocol. If the PIN or password the person enters matches with the one stored in the system, then the person is authenticated.

2. **Something you have**, a secure ID card or other token that can generate a one-time password; a key imbedded in a ‘secure area’ on the host machine, in the browser software, etc; or a smartcard (which may have keys imbedded and can perform cryptographic operations on behalf of a user). This is a token-based authentication. In this scenario, a key is presented in the secure token. Possession of the token means the possession of the key. Therefore, any one who obtains the token can be authenticated as the owner of the token.

3. **Something you are**, such as a physiological or behavioral characteristic. This is a biometrics-based authentication. In this scenario, the biometric is converted into a profile that is compared with a stored profile. Nowadays, the techniques used in authentication include static biometrics, which include fingerprint, retinal, iris, face and hand geometry; and dynamic biometrics, which include voice and signature verification. A person is authenticated if a close enough match is obtained between the biometric and the stored profile. Therefore, the protection of the profiles (by encryption) in transit between the device capturing the biometric and the server performing the biometric check is needed. The information must be protected from capture by a third party who could put it to damaging use, by injecting it into the network.

Token-based and knowledge-based identification objects do not rely on any inherent attribute of an individual to accomplish authentication. There are a number of disadvantages associated with these two authentication methods. Tokens can be lost, stolen, forgotten, misplaced or voluntarily given to an impostor. PIN and passwords can be forgotten, guessed, peeped at or voluntarily disclosed to an impostor. Biometrics are inherently more reliable and do not suffer from these disadvantages. However, they do have other disadvantages, such as being difficult to register, enroll and use; they are also affected by environment and health conditions.

However, all these ‘secrets’ are vulnerable when transferred over the open network; even a hashed password or PIN is vulnerable to dictionary search or exhaustive attacks. Passwords are an example of a weak authentication mechanism; a person demonstrates knowledge of a password matching his/her user ID and the server compares to an entry in a password file. With this sort of password method the password is the secret and the password or a hash of it is revealed.

In strong authentication methods by contrast, one entity proves its identity to another by demonstrating knowledge of a secret known to be associated with that entity, without revealing that secret itself during the protocol. There is no need for two parties involved to know exactly what the password is; it is possible for one entity to get the information associated with that password to approve his/her knowledge of the password. This is the so-called ‘challenge – response’ protocol. It is based on encryption, integrity mechanism (MAC), or digital signature.

4. **PKI/CA**

Cryptographic techniques can be used in concert to provide a complete suite of security services. They should be considered for the protection of sensitive or critical information and systems. Cryptography is a branch of applied mathematics concerned with transformation of data for security. In
cryptography, a sender transforms unprotected information (plain text) into coded text (cipher-text). A receiver uses cryptography to transform the cipher-text back into plain text, verify the sender's identity, verify the data's integrity, or a combination of these.

Digital signature is one of the mechanisms that can be used to protect the authenticity and integrity of electronic documents. It can be applied to any form of document being processed electronically. Digital signature is implemented by using a cryptographic technique based on a uniquely related pair of keys, where one key is used to create a signature (the private key) and the other to check the signature (the public key).

Care should be taken to protect the confidentiality of the private key. This key should be kept secret, since anyone having access to this key can sign documents. In addition, protecting the integrity of the public key is important. This protection is provided by the use of a public key certificate.

One of the principal problems associated with cryptography is to make private keys available to authorized users without disclosing them to any else. Other principal problems include binding the public keys to entities, enabling other entities to verify public key bindings, and providing the services needed for the ongoing management of keys in a distributed system. The emerging approach to address these security needs makes use of the scalable and distributed characteristics of Public Key Infrastructure (PKI). PKI can speed up and simplify delivery of products and services by providing electronic approaches.

The term ‘public key infrastructure’ is derived from public key cryptography, the technology on which PKI is based. It has unique features that make it invaluable as a basis for security functions in distributed systems. Public key infrastructure is the combination of software, encryption technologies, and services that enables organizations to protect the security of their communications and business transactions on networks. PKI integrates digital certificates, public key cryptography, and certification authorities into a complete set of organization-wide security architecture.

A typical PKI encompasses the issuance of digital certificates to individual users and servers; end-user enrollment software; integration with certificates; tools for managing, renewing, and revoking certificates; and related services and support.

5. **PKI Components**

Functional elements of a public key infrastructure include certification authorities, registration authorities, repositories, and archives.

- A Certification Authority (CA), similar to a notary, issues or revokes certificates.
- A Registration Authority (RA), an entity that is trusted by the CA to register or vouch for the binding between public keys and certificate holder identities to a CA.
- A Repository is a database of active digital certificates and certificate revocation lists (CRL) for a CA system.
- An Archive is a database of information to be used in settling future disputes.
- PKI Users are organizations or individuals that use the PKI, but do not issue certificates.

A CA is the basic building block of the PKI, a collection of computer hardware, software, and the people who operate it. It is known by its name and its public key. A CA performs four basic PKI
functions:

1. It issues certificates.
2. It maintains certificate status information and issues CRLs.
3. It publishes its current certificates and CRLs.
4. It maintains archives of status information about the expired certificates that it issued.

A CA issues a digital certificate for each identity, confirming that the identity has the appropriate credentials. A digital certificate typically includes the public key, information about the identity of the party holding the corresponding private key, the operational period for the certificate, and CA's own digital signature. A CA must also issue and process certificate revocation lists (CRLs), which are lists of certificates that have been revoked.

An RA is designed to verify certificate contents for the CA. Like the CA, an RA is a collection of computer hardware, software, and the person or people who operate it. Unlike the CA, an RA will often be operated by a single person. Each CA will maintain a list of accredited RAs; an RA is known to the CA by its name and its public key.

PKI applications are heavily dependent on an underlying directory service for the distribution of certificates and certificate status information. The directory provides a means of storing and distributing certificates, and managing updates to certificates.

An archive accepts the responsibility for the long-term storage of information on behalf of the CA. An archive asserts that the information was good at the time it was received, and has not been modified while in the archive. The archive protects information through technical mechanisms and appropriate procedures while in its care. If a dispute about signature arises at a later date, the information can be used to verify that the private key associated with the certificate was used to sign a document.

PKI users rely on the other components of the PKI to obtain certificates, and to verify the certificates of other entities that they do business with. End entities include the relying party, who relies on the certificate to know, with certainty, the public key of another entity and the certificate holder, who is issued a certificate and can sign digital documents.

6. **PKI Architectures**

Certificate holders will obtain their certificates from different CAs, depending upon the organization or community in which they are a member. A PKI is typically composed of many CAs linked by trust paths. A trust path links a relying party with one or more trusted third parties, such that the relying party can have confidence in the validity of the certificate in use. There are two traditional PKI architectures to support this goal, hierarchical and mesh architectures. A third approach, bridge CA architecture, has been developed to address the problem that organizations face in seeking to link their own PKIs to those of their business partners.

6.1 **Hierarchical**

Authorities are arranged hierarchically under a 'root' CA that issues certificates to subordinate CAs. These CAs may issue certificates to CAs or users below them in the hierarchy. In a hierarchical PKI, every relying party knows the public key of the root CA. Any certificate may be verified by verifying the certification path of certificates from the root CA.
6.2 Mesh

Independent CA’s cross-certify each other (that is, issue certificates to each other), resulting in a general mesh of trust relationships between peer CAs. A relying party knows the public key of a CA ‘near’ himself, generally the one that issued his certificate. The relying party verifies certificate by verifying a certification path of certificates that leads from that trusted CA.

Figure 1.1 illustrates these two basic PKI architectures. In hierarchical, node 1 denotes the root CA.

![Figure 1.1 The Traditional PKI Architectures](image)

6.3 Bridge CA

The Bridge CA architecture was designed to connect organizational PKIs regardless of the architecture. This is accomplished by introducing a new CA, called a Bridge CA, whose sole purpose is to establish relationships with organizational PKIs.

Unlike a mesh CA, the Bridge CA does not issue certificates directly to users. Unlike a root CA in a hierarchy, the Bridge CA is not intended for use as a trust point. All PKI users consider the Bridge CA as an intermediary. The Bridge CA establishes peer-to-peer relationships with different organizational PKIs (Figure 1.2). These relationships can be combined to form a bridge of trust connecting users from different PKIs.

If the trust domain is implemented as a hierarchical PKI, the Bridge CA will establish a relationship with the root CA. If the domain is implemented as a mesh PKI, the bridge will establish a relationship with only one of its CAs. In either case, the CA that enters into a trust relationship with the Bridge is defined as the principal CA.
7. What Is a Digital Signature?

A digital signature is represented in a computer as a string of binary digits. It is computed using a set of rules and a set of parameters such that the identity of the signatory and integrity of the data can be verified. Digital signature is implemented by using a cryptographic technique based on a uniquely related pair of keys where one key is used to create a signature (the private key) and the other to verify the signature (the public key), which is known as Public Key Cryptography.

The digital signature involves two processes: signature generation and signature verification. Signature generation makes use of a private key to generate a digital signature. Signature verification makes use of a public key which corresponds to the private key. Each user possesses a private and public key pair. Public keys are assumed to be known to the public in general. Private keys are never shared. Anyone can verify the signature of a user by employing that user's public key, while signature generation can only be performed by the possessor of the user's private key. The connection between the private key and the public key is so that it is computationally infeasible to derive the signature key from the verification key. Public Key Infrastructure (PKI) facilitates the key management and distribution.

Digital signature can be categorized mainly into three algorithms in terms of generating and verifying, which are as follows.

7.1 Digital Signature Algorithm (DSA)

This is a standard that defines digital signature algorithm (DSA). It was proposed by Schnorr and El Gamal. DSA is based on discrete logarithms for signature generation and verification. A hash function (Secure Hash Algorithm, SHA-1) is used in the signature generation process to obtain a condensed version of data, called a message digest. The message digest is then input to the DSA to generate the digital signature. The digital signature is sent to the intended verifier along with the signed data (often called the message). The verifier of the message and signature verifies the signature by using the sender's public key. The same hash function must also be used in the verification process. Similar procedures may be used to generate and verify signatures for stored as well as transmitted data. In DSA, signature generation is faster than signature verification.

A means of associating public and private key pairs to the corresponding users is required. That is, there must be a binding of a user's identity and the user's public key. This binding may be certified by a
mutually trusted party. A Trusted Third Party (TTP) is involved to resolve the problem of disputes. For example, a certifying authority could sign credentials containing a user’s public key and identity to form a certificate.

7.2 RSA Digital Signature Algorithm (RSA)

This signature scheme is based on RSA public key encryption algorithm. RSA is named from its inventors who are Rivest, Shamir, and Adleman. The security of this signature algorithm relies on the difficulty of factorization of large prime numbers. There is a publicly known number $N$ that is the product of two primes, whose values are secret. These primes are very important, because anyone who knows their values can use them to calculate the private key from the public key. However, the signature generation and verification process are more or less same as DSA. Using RSA digital signature, the verification of a signature is much faster than signing. This is desirable because a message will be signed by an individual only once, but the signature may be verified many times.

7.3 Elliptic Curve Digital Signature Algorithm (ECDSA)

Elliptic curve cryptosystems were first proposed independently by Victor Miller and Neal Koblitz in the mid-1980s. The main attraction of elliptic curve cryptosystems over other public key cryptosystems is the fact that the security of elliptic curve digital signature relies on the underlying hard mathematical problems: Given two points $G$ and $Y$ on an elliptic curve such that $Y = kG$ (that is, $Y$ is $G$ added to itself $k$ times), find the integer $k$. This problem is commonly referred to as the elliptic curve discrete logarithm problem.

Elliptic curve cryptosystems have emerged as a promising new area in public key cryptography in recent years due to their potential for offering similar security to established public key cryptosystems with reduced key sizes. They are especially useful in applications for which memory, bandwidth, or computational power is limited. Elliptic curve cryptosystems with a 160-bit key offer the same security as the RSA system and discrete logarithm-based systems with a 1024-bit key. As a result, the length of the public key and private key is much shorter in elliptic curve cryptosystems.

However, it is misleading to describe the signature algorithms as ‘encryption with a private key’. The symmetric algorithms, in which the same key (known as the secret key) is used for both encryption and decryption, can also be used in the signature generation process. In this case, a secret channel needs to be set up to distribute the secret key to ensure the confidentiality of the key transmission. The asymmetric algorithms are used to facilitate the key distribution, where the key-pair is used to encrypt and decrypt the secret key (here the key is known as key encryption key). This is useful when the message is arbitrarily long. Symmetric algorithms can speed up the encryption process, while asymmetric algorithms can ensure the secret distribution of the encryption key, data integrity and non-repudiation.

8. How Does Digital Signature Work?

The purpose of digital signature is to provide a means for an entity to bind its identity to a piece of message. The process of signing entails transforming the message and some secret information held by the entity into a tag called a signature. For digital signature to be useful in practice, it must

- Be easy to compute by the signer, which is to say, the signing function should be easy to apply.
- Be easy to verify by anyone, which means the verification function should be easy to apply.
• Have an appropriate lifespan, which means that the digital signature must be secure from forgery until the signature is no longer needed for its original purpose.

The signing and verifying process can be outlined as follows:

1. **Possession of Public and Private Key Pair.** At the beginning of the transaction or during the transaction, the participants must acquire one another's public key, while the private key of either party must keep secret.

2. **Generation of Message Digest.** The sender uses a hush function, which is a one-way algorithm, to transform a message into a fixed-length value. This fixed-length value is known as message digest.

3. **Signing the Message.** The sender uses his private key to encrypt the message digest, which forms a signature of the message. This signature is then appended to the message.

4. **Message Sent.** The digitally signed message is sent ‘in clear text’ to the recipient. Because any change made to the content of the message will result in a non-match of the received hush value.

5. **Message Verification.** The recipient will generate a hush value from the message received with the same one-way hush function. The encrypted message digest can be decrypted with the sender’s public key. Then these two hush values will be compared. If the two values match that means the message is genuine and authentic; if the two values do not match, this indicates possible impersonation, message alteration, or an error in transmission.

6. **Message Encryption (optional).** The entire message can be encrypted with the recipient's public key to ensure the confidentiality of the message content.

7. **Message Decryption (optional).** The message can be decrypted with the recipient's private key.

8. **Time Stamping.** A time stamp can be used to trace the transaction, in case a dispute arises in the future.

However, in the case of the message being very short, there is no need to transmit it separately, because it can be recovered from the signature itself.

9. **Benefits and Risks of Using Digital Signature**

   Increasingly, organizations are attempting to automate paper-based processes. The benefits of using digital signatures may be obvious, while there are also some potential risks. Benefits include

   • **Greater efficiency in document processing.** Documents transmitted electronically with a digital signature reduce paperwork, travel, and delays in processing and delivery costs. These benefits become more pronounced as the number of transactions increases.

   • **Enhanced services.** Digital signature provides strong authentication that allows the agency to supply broader services and to promote its administrative goals and objectives to a wider audience. In effect, a government can serve the public 24 hours a day, seven days a week.
• **Document source is verifiable.** Anyone can use the public key of the signer to verify the correctness of the signature at any time without any consent or input from the signer.

• **Reduced possibility of fraud, forgery and impersonation.** It is virtually impossible for a person to forge a signature because only the signer knows his private key.

• **Improved integrity of documents.** Any changes made to a message will invalidate the signature. Thus, it is impossible to copy a digital signature from one message to another.

The risks associated with the use of digital signature are

• **Lack of legal specification.** No well established specifications exist to indicate where digital signature is legally acceptable for which type of document and to what extent an agency requires a digital signature versus another form of identification.

• **Connective to existing agency infrastructure.** The application and PKI have to function well across security systems, access control devices such as firewalls, and other information processing systems.

• **Interoperability with other agency infrastructures.** The ability to accept some other mechanism of PKI is necessary so that a user in one PKI domain can be accepted as a trusted user in another PKI domain.

• **Standard archiving.** When a digitally signed document is in equivalence with an ink-signed paper document, there is a requirement for standard archiving to make sure it is as accessible to inspection as in the case of any paper-based legal document. The archived document must be available whatever software and hardware updates occur.
1. Introduction

The advent of e-commerce has meant that payment systems must cope with new requirements. With the widespread use of the Internet, e-mail, and mobile phones, payment via electronic means provides greater convenience and choice in payment services. The growing need for solid and robust electronic business and payment systems has made e-payment proliferate as a payment method in the past few years. E-payment plays a key role in e-government development as well, because many transactions need to be settled electronically when government does business online.

2. What is e-Payment?

E-payment is slowly but steadily growing in most countries. It is about paying online for goods/services. A number of institutions and businesses have woken up to the idea of offering their goods/services online in a secure way to reduce their operational costs. To understand electronic payment, it is useful to consider first the traditional methods of payment.

2.1 Cash

Cash is the most widely used and dominant method of payment in all countries. It requires face-to-face interaction between a customer and merchant. Normally it guarantees payment directly. However, this method is not suitable for large payments, and leaves no audit trail.

2.2 Cheques

This involves a payer's bank issuing a chequebook. When there is a payment request, the payer (customer) presents a cheque to the payee (merchant). Then the payee presents the cheque to their own bank, where the cheque will be forwarded to the payer's bank for clearing. The payer's bank verifies the availability of funds and debits the account of the payer. This method is suitable for any value of payment. The payee can be remote from the payer, and the payer gets a few days of grace before payment. However, this method of payment has a high rate of rejection (the bouncing problem), and the processing cost is high (usually 20 cents to $1 per cheque in the United States).

2.3 Credit Transfers (Giro)

In this method, the payer instructs their own bank to initiate a payment usually by sending a Giro to the payer's bank. The payer's bank verifies the availability of funds, debits the account, and forwards them to the payee's bank for clearing. The transfer only occurs if the payer has sufficient funds. The payer can choose the precise date of transfer.

2.4 Bank Cards

Payment with bankcards is highly convenient, and it is suitable for any value above about $2. This is sometimes called off-line electronic payment and involves the following ten steps:
1. A payee (merchant) applies to a bank (acquiring bank) for a merchant service, which allows the use of the bank's credit and debit cards at his/her place of business.

2. The merchant negotiates the associated costs with the acquiring bank.

3. On acceptance, the merchant pays the set-up costs.

4. The merchant receives and installs a PDQ machine, which is used to 'swipe' credit and debit cards.

5. The merchant 'swipes' the customer's card to collect their credit or debit card details.

6. The card details are passed to the acquiring bank for approval. The acquiring bank checks the details of the card and authorizes the transaction.

7. The merchant asks the customer to sign the sales voucher.

8. The merchant verifies the signature and processes the payment.

9. A transaction charge is automatically paid to the bank by the merchant.

10. The customer leaves with the goods or service.

However, the e-payment which will be discussed most extensively in this module is online electronic payment. On-line methods can be divided broadly into those that are mostly based around the Internet, those based on mobile phones, and those using pre-paid cards.

3. Internet Based Payment

There are a number of ways to carry out a payment by the means of the Internet, which are described as follows.

3.1 Plastic cards

These are the predominant means of payment for Internet shopping, particularly in the form of credit cards. The Internet is used as an access channel for card transactions. An Internet Merchant Service ID is required for this scenario, and a virtual PDQ is used to swipe the customer's card. In this way, the card details are collected over the Internet and forwarded to the acquiring bank. Nowadays, cards are adapted in significant ways for more secure and convenient use in the Internet environment; for example, smart cards embedded with a user password enable financial institutions to authenticate the users and to validate cards used for online payment.

3.2 Account-based e-Payment

This method facilitates person-to-person payment. Some businesses use it as a means for customers to pay online. A pre-funded e-payment account with the service provider is required before making an 'instant' payment to another user. The sender of the funds only needs to know the recipient's email address, not the full bank details. However, the recipient of the funds must join the payment service to accept the money.
3.3 Other email/online payment

There is no need to set up a separate e-payment account in all instances. Instead, an Internet service can ‘overlay’ existing banking arrangements to offer an online bank account to receive account transfers. Similar to account-based e-payment services, the sender only needs to know the recipient’s email address to initiate a transfer. This is more like an access channel to existing payment arrangements and has more in common with online banking.

4. Mobile Phone Based Payment

As mobile phones become popular, they have been increasingly used as the methods to implement e-payment and have been extensively accepted by dealers and customers.

4.1 As an access channel

A mobile phone is a convenient access mechanism for payment against traditional payment. It is usually categorized under the heading of m-payment. In this case, the mobile network operators offer services that allow users to charge purchases directly to their payment cards that they have pre-registered with the service.

4.2 Reverse charging, or ex-post billing

In this case, payments for goods or services are placed as additional items on the customer’s post-paid phone bill. The bill is then paid in a normal way. The phone company records all payments, including customer and merchant details, and sends the merchant a consolidated payment periodically.

4.3 Premium-rate services (PRS)

This method allows a purchase to be made by routing the purchasing call through a premium-rate number. The cost of the call includes both the call itself and the amount of the goods/services purchased. Typically, the caller’s phone company routes such calls to another phone company which then either provides the premium-rate service itself or may also pass the call on to another supplier. The revenue from the caller is divided between the various parties of the transaction. The charges can be paid for by either using pre-paid airtime or ex-post billing arrangements. This is also applied to fixed-line phones.

4.4 Pre-paid airtime on a mobile phone

Pre-paid airtime can be used to pay directly for non-telephone items from third parties. This is suitable for users without bank accounts or credit cards. The phone company collects the funds from the user to pay for airtime in advance of the transactions. When a user makes a purchase, the phone company can retain the part that is its own revenue for the phone call and pays the merchant what is due for the goods/services purchased.

Premium-rate services and pre-paid airtime on mobile phones are suitable for low-value purchases and are known as micro-payment. They must necessarily be lightweight. Otherwise the charges may exceed the purchase value.
5. **Prepaid Cards/e-Purses**

These schemes were generally called e-money. They have the longest history among e-payment services and are also aimed at low-value transactions. The e-purse scheme operator takes conventional money from card users in exchange for a card loaded with the same amount of value. Retailers accept the cards in payment for goods/services ultimately receiving conventional money from the scheme operator.

6. **E-Payment System**

The Internet as an open network infrastructure has several implications for the way e-payment systems function. Traditional banks remain the ‘backbone’ of e-payment systems. This implies that all payment solutions depend to a certain extent on the efficiency of payment systems run by banks. At the moment, the flow of payment remains bank-based. All network operators have a close working relationship with the banking sectors. Many new payment mechanisms have been developed for payment on the Internet, for example, Secure Electronic Transaction (SET) has attempted to make online payment safer by adding security measures. Furthermore, the picture is made more complex by the wealth of payment methods being linked to an increasing number of communication channels that can be used for electronic payment. These include POS transactions, e-commerce, and m-payment with mobile phones. Different access channels, such as WAP access to the Internet or digital TV for online shopping make the possibilities of e-payment more vivid and significant.

E-payment architecture should provide a flexible and extensible structure to accommodate payment requirements on the Internet. It should support and enable the full cycle of payment transactions in which open Internet payment protocols are integrated with existing and future payment systems used by financial institutions. Whichever form the e-payment methods take, the structure of a bankcard based e-payment system is illustrated in Figure 1.1.

![Figure 1.1 An Example of an e-Payment System](image)

However, the continued development of applications and the continued availability of human resources are vital for the success of e-payment systems and their continuing growth. A secure and user-friendly e-payment system leads to a largely homogeneous payment method. An e-payment
system will have specified core function with additional features to cope with variation and diversity. Gradually information technology will make the technology of the traditional payment methods, like cheques, credit transfer or direct debit obsolete.

Developments arising from the competition that exists between different networks are making e-payment an ever more convenient and trustworthy payment method for users. At the moment there seem to be a particularly strong drive towards integration. Non-banking institutions, such as telecommunication operators, ISPs, or software firms, are moving into the area of financial services (including payments). At the same time, banks are offering more online services to their customers. In addition, representatives from both sides are working together to construct the national Public Key Infrastructure to ensure the security of the e-payment system.

The interoperability between different payment systems makes e-payment more successful. In addition, the integration of those processes involved in a business transaction, such as ordering, billing, offers and receipts, together with the payment process itself, forms a harmonized architecture for the e-payment system.

7. Risks Related to e-Payment

Many people feel unsafe paying through the Internet for goods/services. This is due to the sensationalized reports in the media about the use of fake credit cards for unauthorized transactions. However, negative aspects and consequences of Internet payments do exist. These can be divided into two main categories: loss of money and loss of privacy. Loss of money refers to financial loss experienced by customers, merchants or service providers. Loss of privacy refers to information that customers prefer to keep private becoming available to others. Therefore, the risks related to e-payment are

- **Disclosure of confidential information.** One of the foremost concerns related to e-payment. Information such as personal details, credit card numbers or passwords can be obtained by intercepting network traffic or by unauthorized access to the computers that are connected to the Internet. This information can be used to make a false transaction that causes either loss of money or loss of privacy.

- **Disruption of service.** A result of a system malfunction, such as hardware/software becoming unreliable, or of systems being compromised by a virus or a hacker, eventually leading to the loss of money.

- **Usurpation.** Refers to different methods used to take over the privileges of others in order to misuse them. Hackers with special tools can access the system to manipulate data so as to alter an account balance. This could lead to both loss of money and loss of privacy.

- **Illicit modification of payment information.** Refers to altering existing data in the payment system that could lead to a misdirection of payment, an imbalance of the e-purse, or a disruption to the system data that effects the audit trial.

- **Counterfeiting.** Refers to those activities that create new data structures, which are technically valid but not legally admissible, such as the creation of a fake account or payment transactions. This could lead to either loss of money or loss of privacy.

- **Transaction replay.** Refers to the replay of a payment transaction, which causes repeated debiting of an account or the re-use of e-money. This could happen when a person familiar with the payment system’s transaction format has intercepted the
transaction database.

The risks related to e-payment are still low in comparison with traditional payment methods. Initiatives introduced by the card payment industry to protect the customer, merchant and card issuer have made e-payment more secure than ever.

In order to maintain a secure environment for online trading over the open network, it is necessary not only to replace the traditional face-to-face mechanisms with new electronic ones but also create new tools to manage the specific risks associated with e-payment. Public Key Cryptography (PKC), Public Key Infrastructure (PKI), and digital signature are the most commonly used mechanisms to ensure a secure and trustworthy environment for e-commerce as well as e-government. A detailed discussion on these mechanisms can be found in other modules.
1. Introduction

Portals have the ability to support the overall goals and objectives of an organization. The return on investment in them is usually possible through an increase in general productivity. Consequently, a well-deployed portal has become increasingly important to an organization’s daily operation. Portals are becoming the preferred way for an organization to allow customers to see aspects of their internal operations, and to improve transparency for employees and partners. At the same time, portals allow customers to conduct their business with an organization in an automated fashion. The essential aim of e-government is to build government for the information age. Although people may not actually know exactly what the government of the information age will look like one thing is clear -- the front door of a government is, most probably, its portal.

In this regard, a government portal has become increasingly important in allowing citizens to access government information easily and to enjoy one-stop government services. A well-developed portal will complement and enhance customer-focused channels which may already exist in a government. For many government websites, portals are becoming the main source of cross-agency and high-value services to clients. Because technology has the ability to store and organize information, a comprehensive, one-stop service has become the acceptable and required standard.

In the early stages of online government, websites were designed with the existing structure which placed government at the center. Computer screens were organized to reflect the organization of the government. However, users are not usually interested in how the government is organized. Instead, they are concerned with how they can effectively access the government services they want or need. Government online portals that reflect the government structure can be considered to be government-centered rather than citizen-centered. Such portals are not taking full advantage of the opportunities provided by modern technology.

2. What is a Portal?

A portal allows an organization to present information, applications and services in a single consolidated browser view. A portal provides a secure and individualized view of multiple online resources and interactive services. It offers a single access point to critical information and the primary applications necessary for an individual to perform daily business operations with the organization. In this sense, a portal becomes an interface between the government and the citizens. In fact, with the advent of the information age and the development of e-government, the interfaces between government agencies and between governments and their citizens are shifting from the traditional ones, such as offices, windows, counters, concierges, etc. to an electronic one, i.e., portals.

Portals have been deployed to solve many types of business problems. Some portals are built as dashboards, providing indicators which contain all the key performance indicators that relate to a particular role and which need to be understood by the role holder and others with an interest in it. Generally speaking, a portal has the following functions:
• To address a narrow business problem or business opportunity.
• To support a specific business function.
• To target specific audiences.
• To support self-service functions.
• To support general productivity.

Therefore, a portal can be used to eliminate the need to navigate multiple websites and applications so that users can access the different information and services required to do their jobs or to carry out a business transaction. A well-deployed portal presents a personalized view with a logical organization and grouping of information that leads to an increase in productivity. It offers a broad range of capabilities to allow organizations to quickly link individual applications without composite programming. A portal is a mechanism that extends the reach of an organization to a broad range of audiences both internally and externally.

3. Portal Deployment Rules

Organizations should deploy portals wisely to achieve productivity savings and a competitive advantage. Wise portal deployment can help organizations achieve millions in productivity savings, accelerate critical business activities, and provide a competitive advantage by broadening the scope of access to content, applications, and business processes to key customers and trading partners.

The most important portal deployment rule is to improve the relevance of services in line with the needs of users. That is to say, the needs of different users and user groups must be considered separately. Providing more effective access to specific information or an application can make a meaningful difference to a user's work outcomes or service experience. If a portal does not achieve this for a critical number of users it may be little more than an expensive irrelevance.

Organization portals must be deployed in the context of a comprehensive portal strategy. This strategy should be part of an organization-wide IT strategy that is sponsored by the business. Therefore, it is vital to identify the portal's connection to the organization's business goals and objectives, while striving to quantify pragmatic and tangible benefits. Organizations should manage their portals from a holistic, federated environment to receive the highest returns on information access and collaboration.

Portal interoperability should also be taken into consideration. Governments often have to manage more than one portal. If the services are from different government agencies, operating relatively independently, the problems of interoperation between them may create a significant problem for portal management. In the short term, this can be solved by integrating directory, security, personalization profiles, metadata, and portal components. For the long term, portal interoperability standards are needed for providing full interoperability across portals provided by the different government agencies.

In addition, the integration of portals with state of the art or best-of-brand, third party products should be leveraged. Nowadays, portals function increasingly through technologies such as search, content management, and collaboration. Although these functions will be maintained and new features added. Features such as composite applications, extension to personal content, use of portal-enabled application servers, and federated portal functionality across different departments of a government. Portals will become a technological convergence center for many complementary technologies.
Portal deployment should be in an incremental fashion that can be continually tailored to the complex requirements of government. It is better to think strategically but implement tactically. It is likely that the requirements and the understanding of the requirements may improve over time. While keeping in mind the overall mission, goals, architecture and standards, portal deployment should be done one unit at a time and through a detailed discovery of requirements for each unit.

Finally, governments should develop solutions that incorporate a portal ecosystem. Portals will facilitate a new generation of composite applications. Portals are a natural fit for many composite applications by providing a starting point for development, and by providing facilities for integration and user interface management and administration. Those composite applications will enable governments to fuse internal business processes with those of business partners.

4. Leverage Portal Projects

A portal has many benefits for an organization. It can greatly accelerate the speed of business and throughput, and can also reduce the time it takes to make and implement decisions, while helping to improve the overall quality of the decision making process. Through the development of portals, the naissance of some new concepts of e-government has become possible; concepts such as 24/7, one-stop service, non-stop service, and so forth. Hence, a well-deployed portal is significant to the success of e-government, and government managers will therefore be interested in, and benefit from, guidance on portal deployment.

Portals may succeed or fail. Six categories of success and failure have been identified from experience. They are

1. **Catastrophic failure.** A catastrophic failure is one in which the negative impact to the organization rises above the costs of software licenses and resources used for deployment, through some chain of circumstances that leads to bad business decisions based on incorrect information. However, few portal projects fall into this category.

2. **Shelfware.** In a shelfware scenario, a portal project fails but the impact is limited to the cost of the portal and opportunity cost. A portal’s implementation may be classified as shelfware from an organization’s or a vendor’s point of view if the portal procurement is approved, the vendor is paid and the license is secured, but the project never proceeds beyond that stage. A variation of shelfware is a proof-of-concept deployment that does not proceed. It is estimated that 20% to 50% of organizational initiatives fall into this category.

3. **Teflon portal.** This is most common mode of failure. In this mode, the portal project appears to be successful at the first stage, as it is implemented exactly on schedule, and all components that were identified in the initial requirements are in place and basically work well. However, users of Teflon portals do not return after the initial excitement has worn off. The bottom line is that the portal investment is underutilized, which is often not immediately obvious. Analyzing usage metrics can bring this kind of failure to light.

4. **Modest success.** Modest success and Teflon failure are difficult to distinguish through casual observation, as both portals might look the same, have similar functions, and be equally invisible to the organization. The way to distinguish failure from success is through analysis of usage metrics. A portal project is said to be a modest success if there are users who rely on the portal, but they do not find the portal compelling or essential. The situation is not static because a modest success portal project can slide into an invisible failure if insufficient attention is paid to content updates, feature enhancements, and requirements
5. **Visible success.** A portal project can be put into this category if it changes the way people conduct their daily activities or common tasks. A visibly successful portal will transform certain tasks, job roles, and processes. For example, it can automate some tasks that were previously accomplished manually, so that information is delivered in a more efficient and cost-effective way. A visible success portal project will include functional integration with core business applications, plus a range of self-service portlets.

6. **Resounding success.** If a portal project exceeds even the highest expectations, then it is called a resounding success. In this scenario, the portal forms a key part of core business processes and brings significant benefits to the government or to business. The government’s competitive position is strengthened as well. However, less than 1% of organizations are reported to have achieved resounding success in portal projects.

Generally speaking, the majority of portals are partial failures and partial successes. Nevertheless, the overall percentage of successes outweighs the failures. Portal managers should identify appropriate criteria to assist in distinguishing between success and failure. In the interim, the development of certain indicators to measure the success of a portal is to be encouraged. In the state of Minnesota, USA, one measure is to assess how many people have bookmarked North Star as their home page. Other measures include a more engaged citizenry and improved trust in government.

5. **The Role of a Portal**

A Government portal is a multifunctional tool, from which many services and communication systems are accessed. Government portals are able to provide many capabilities including

- Aggregating both internal documents and external content feeds into one or more repositories.
- Making the content accessible through a search engine.
- Rationalizing the user interface through presentation management.
- Providing personalized access for users.
- Providing a robust, reliable framework for portal components or portlets.
- Allowing portlets to access enterprise data and business logic through integration technology.
- Providing a single sign-on mechanism for integrating access and authorization.
- Providing coexistent and interoperable multiple portal deployment.
- Enabling various degrees of centralized and delegated management and administration.
- Supporting a range of collaborative mechanisms.

Government portals are used as a gateway to support and enable the real-time operation of the organization. The goal is to provide an environment in which work and activities can be accomplished inside the portal. Deployed at the level of the organization, portal project initiatives may include portals
for: knowledge management (KM); business intelligence (BI); business activity monitoring (BAM); and enterprise content management.

6. Five Steps to Real-Time Organization

Government portals can greatly facilitate the organization's real-time operation. They support strategic goals and allow for the establishment of finer-grained, better-tailored operational goals. Portals can provide both surface and deep level correlations across applications and systems. It is believed that a successful real-time organization process consists of five steps.

6.1 Setting Goals

The first step towards a real-time organization operation is affirming organizational goals or establishing new ones. These goals can be general or strategic, as well as narrow or tactically focused. An organization's portals should support these strategic goals.

6.2 Designing

Identification or re-validation of the metrics that directly relate to organizational goals and objectives is the starting point for designing portals. Most metrics will be shared between portals and other real-time organizational operation-related initiatives. In a discussion or consultation, for example, the portal can provide metrics relating to the number of ideas discussed, number of participants, elapsed time for the discussion phase, and the number of follow-on ideas generated.

6.3 Constructing

Portals can be used to implement business logic that refines and transforms low-level data into high-level metrics. The organization's infrastructure should be constructed in such a way that raw data for the relevant metrics can be captured easily. Metrics generated by other systems can also be made available to users through portlets. The common approach is the use of thin high level metrics, rather than thick masses of lower-level data.

6.4 Implementing

Portals can serve as both the principal and multi-channel delivery mechanism for metrics and actionable content. They can also provide principal mechanisms for decision makers to take action on the delivered content. Portal components are usually in a read-only query and as a reporting system but are not restricted to a one-way flow of information.

6.5 Continuing Management

Portals provide a link to cross boundaries between applications and infrastructure by expanding the audience for information delivery, increasing the depth of available content, providing a comprehensive and consistent user interface, and by providing tools for personalized access.

7. Trends of Government Portals

While portals are currently at the center of most governments’ immediate e-government strategy, they are also an important initial step towards an overall long-term strategy. Portals provide constituents (i.e., citizens, businesses, and governments) with a front door to seamless interaction with their government. Many governments refer to the need for a central, up-to-date catalogue of government
services to enable citizens to see the big picture in a single location and portals can provide this.

Close attention to branding is essential. All governments have committed valuable resources to the development of their portals. When the various levels of government begin to integrate, the identity of each entity becomes critical.

As mentioned previously, in the early stages of government portal development, portal designed was based on the government's organizational structure, i.e., they adopted a government-oriented approach. However, the developers soon discovered that the users are not interested in how the government is structured. Instead, they are concerned with finding the services they want or the answers to their questions. As a result, portals are now designed using what is referred to as the 'client-centered' or the 'demand-oriented' approach. A number of different models have been developed to do this. For example, the audience, such as citizens, businesses, entrepreneurs, civil servants, or non-citizens (tourists for example) may become the primary categories and gateways on the initial portal page. Canada and the Netherlands have found this to be their preferred model. Another model, used by Singapore and numerous state governments in the United States, is the life event model based on key events such as birth, education, entry or exit from work, marriage, or the need to provide or receive care. In addition, portals are being developed for communities of interest such as seniors, students, farmers, and workers or by a functional area such as disaster reduction. Large governments such as the United States and Canada have implemented this approach.

Governments are designing portals using a complex enterprise architecture that encompasses many technologies, navigation methodologies, and features. A directory of services organized by topics along with advanced search capabilities provides a mixture of navigation options to users. The use of geographic information system (GIS) capabilities provides the user with the ability to personalize the site. The State of Washington has incorporated a feature entitled ‘Ask George’ that allows the user to ask English-like questions and to receive a response much like the popular ‘Ask Jeeves.’ Some governments have employed other types of dissemination technologies that will move portals to the next level of maturity. These include interactive voice response (IVR), kiosks, and wireless devices.

Portals are being built to be scalable and to avoid significant and costly upgrades as they accommodate future growth and shifts in technology. Innovation through the introduction of features such as a catalogue of government products and services and personalization are also important trends. Portals have undergone and will continue to undergo a maturation process. As Arizona in the U.S. has identified, portals offer a powerful method to build end-to-end integration and to move transactions online. We are, without a doubt, in the infancy stage of e-government. Full maturity will only occur with strong leadership and commitment from both the executive branch and the legislature combining to create a well-coordinated e-government strategy that provides incentives for collaboration. Currently, many governments, through portals, are well on their way to a new plateau of excellence in e-government.
Change Management

1. Introduction

Organizations have to initiate change processes in order to meet market demands, to increase shareholder values, or to fulfill government strategies. They often have to initiate and apply change processes to maintain organizational stability and to support balanced economic growth and sustainable development. Change management is a process that enables an organization to modify any part of its structure so that it can effectively deal with the constantly changing environment. It includes activities designed to secure support, acceptance, and approval for the necessary and agreed modifications and changes. The purpose is to control changes while preserving the integrity and service quality of the production environment. The concept and practice of change management has become increasingly popular among organizations in recent years.

As indicated in previous modules, e-government is not simply the computerization of current government business but, instead, a transformation of government. It is a reconstruction and a re-engineering of government that brings with it significant change. Therefore, effective change management is certainly a big challenge, and probably a necessity, for all the governments that are carrying out e-government implementation.

2. Resistance to Change

The rate of implementation of any new technology within a large organization is often dramatically slow. The following paragraphs discuss some of the reasons why.

2.1 Fear of Technology

In many instances, the resistance to change is because high level or senior officers of an organization have little or no knowledge of new technology and are afraid that they will lose their predominant position, supported by the old management system, to those officers who understand the new technology better than they do. This becomes a critical issue if the people who fear the new technology or change, are those who have the power to enhance government informatization and the e-government systems development process. Only determination and pressure from higher authorities can improve the situation.

2.2 Creative Habits

Once people become accustomed to an established way of doing things, they have a natural tendency to resist new approaches. This is understandable because it is human nature to feel comfortable with what they know. However, if this behavior is not properly controlled, it can degenerate into a serious attitude problem where people stay anchored in the past and systematically refuse to grow and learn new approaches.
2.3 Insufficient Time to Learn New Techniques

There has indeed been a large increase in the number of sophisticated application systems that must be developed and implemented to satisfy the needs of users, often with limited resources and time. This naturally creates constant pressure on systems developers and providers who are also under pressure to deliver as many direct hours as possible to the users. The net result may be that those operating or providing the new systems, tools and techniques have inadequate time to learn about them. In some organizations, insufficient time results in staff not receiving any formal training.

2.4 Competing Techniques

Many new techniques emerge year after year. In some instances, they compete against each other. It is not uncommon to be faced with many techniques that in fact are quite similar but use slightly different terminologies. It is not much of a problem to opt for one as opposed to another. Rather, the problem arises when each has its own champion. If not properly managed, the selection process for the acquisition of new tools and techniques can turn out to be not as straightforward as it should be, even though sound selection criteria were used in the process.

2.5 Environment Compatibility

Many of the productivity tools introduced within system development work best when they are primarily used to develop new systems. However, the introduction of a new system into the existing maintenance world may take longer because they might not be readily fully compatible with the existing maintenance and operational environment.

2.6 Built-in Obsolescence Syndrome

New products come to the market every day as a consequence of the rapid development of information technology. Each product brings some enhancements to provide a better way of doing things when compared with previous similar products. An attitude problem surfaces when the decision to bring in a new tool is delayed until the following year because something better will most likely come along. A year later, the same decision is delayed for the same reason. The same scenario can occur with methods. Thus, irresolute and hesitant decision making also contributes to a resistance to change.

This identification and introduction of factors causing resistance to change, shows that developing a new e-government system is not a straightforward process, and that maintaining and operating an e-government system may need considered and considerable effort.

3. What is Change Management?

There are three basic definitions of change management. The first and most obvious definition is that the term refers to the task of managing change. Managing change is itself a term that has at least two dimensions:

The first dimension deals with the making of changes in a planned, managed, systematic fashion. It aims to implement new methods and systems in an ongoing organization more effectively. The changes to be managed lie within and are controlled by the organization. However, these changes might be originated by outside events.

The second dimension of managing change covers the response to changes over which the organization exercises little or no control; changes resulting from activities such as legislation, social
and political upheaval, actions of competitors, shifting economic tides and currents, and so on.

The first and second dimensions are typically characterized as being proactive and reactive respectively.

Change management can also refer to an area of professional practice and this is the basis of the second definition of the term. Independent consultants can act as change agents to help their clients manage the changes they face, or to help them to take a proactive approach to change by taking on the task of managing unavoidable change. In almost all cases, the process of change is treated separately from the specifics of the situation. Professional change agents undertake the task of managing the change process by working with organizational managers and users who know the specifics.

The third definition of change management is based on the content or the subject matter. This consists chiefly of the models, methods and techniques, tools, skills and other forms of knowledge that go into making up the practice of change management. These component bodies of knowledge are linked and integrated by a set of concepts and principles known as General Systems Theory (GST).

4. Change Management Benefits

The benefits of change management are plentiful and are mainly associated with reducing risk and improving service quality. Change management is required for achieving a high degree of IT availability and service quality. Through effective management of the change process both unplanned and planned downtime can be reduced. Thus the quality of service is improved, IT support and business downtime costs are reduced.

Change management can improve the effectiveness of communication. Better communication between users and an organization will result in a greater understanding of each other's needs and priorities, whilst highlighting the fact that business units do not operate in isolation. With increased communication, input and availability, users will feel more empowered and less frustrated when systems are down for maintenance.

Change management can simplify and support the timely flow of information and operations. The process of change will help organizations to streamline the flow of information to simplified levels for 'real world' use, maximize existing software utilization in order to decrease useless reports and to improve productivity.

The creation of a series of analyses that can be used to achieve product/service cost reduction is another benefit of change management. This can help the organization to increase and target revenues and profits. These analyses include product cost analysis and job cost analysis both of which are useful for service decision-making. They also include the matching of actual to estimated costs, direct labor utilization analysis, and corrective measures and actions.

However, change management is one of the hardest management disciplines to implement. It requires a large cross-functional team of application, operational and business people whose focus is on the end-to-end business service and individual component change. It needs a parallel configuration management project to define the relationships among business processes, IT services, and underlying applications and infrastructure.

Change management is also difficult because it involves changes to people's behaviors. Reshaping people's behavior requires a significant amount of education to raise awareness and to bring new competence. To change organizational culture and habits cross-departmental teamwork and collaboration is crucial to success. Furthermore, support by senior management is also needed to
reinforce the importance of change and to emphasize the adverse consequences, for the employees as well as the organization, of breaching the process and failing to adapt.

5. Change Management Process

Change management is a process of problem finding and problem solving. Managing change is a matter of moving from a problem state to a solved state. Three types of goals and activities are involved to transform, to reduce, and to apply. The transformation of goals and activities is concerned with identifying differences between the two states, the problem state and the solved state. The reduction of goals is concerned with determining ways of eliminating these differences. The application of goals is concerned with putting into play operators and activities that actually eliminate these differences.

A problem is usually identified as a situation requiring action for which the required action is not known. Hence, a search for a solution is required. In other words, a search for a course of action will lead to the solved state. This is known as ‘problem solving’. The search for situations requiring action is called ‘problem finding’. In combination, the two activities (finding and solving) help to identify and settle on a course of action that will result in the desired and predetermined change in the situation.

Stating and defining the change problem is at the heart of change management. In this process the future state will be identified, the current state will be described and defined, and decisions about the structured, organized process for getting from one state to the other will be taken. The earlier a change is considered, the better the participants are able to plan and to recognize the effects and risks that may not have been considered in the project plan.

Defining and stating the change problem includes providing answers to ‘how’, ‘why’ and ‘what’ questions. The initial formulation of a change problem often centres on the means of change. It is often expressed in the form of a ‘how’ question, with the goal state more or less implied. By contrast a focus on the outcome introduces a ‘what’ question. Answering the ‘what’ question requires a diagnosis of the problem and a discussion about the end sought. ‘Why’ questions should be answered in order to reveal the ultimate purposes of functions and to open the door to finding new and better ways of performing them. Together, these questions can find the ‘true’ ends, or outcomes, of a change effort.

Three basic stages of the process of change management are usually recognized. They are unfreezing, changing, and refreezing. This view adopts, and derives from, the systems concept of dynamic stability. That is to say, the beginning and ending point of the unfreeze-change-refreeze model is stability.

6. Skill Requirements

Unusually broad and finely honed sets of skills are required to manage change within an organization. These include

1. **Political skills.** Organizations, as part of social systems, can be intensely political. An organization has to make its own judgments as well as own, approve, and accept the change process. This can not be done on behalf of the organization.

2. **Analytical skills.** An ability to analyse workflow operation, within systems, and an ability to undertake a financial analysis are two particularly important sets of skills. Determining the financial and political impact of changes to operations and systems is an important skill for change agents.
3. **People skills.** People are the basic factor of any organization. They vary in national origins, religious beliefs, intelligence and ability levels, attitudes toward life and work, and so on. Therefore, communication or interpersonal skills are needed to develop a better understanding of the diverse individuals within an organization and the part they can play in change.

4. **System skills.** A system is an arrangement of resources and routines intended to produce specified results. In this case, a system reflects an organization, and an organization is a system. There are two sets of systems knowledge and skills to be mastered; they are systems analysis and General Systems Theory (GST). These deal with both the ‘closed’ and ‘open’ systems that carry out organizational goals and objectives.

5. **Business skills.** Understanding how a business works will entail an understanding of finances and money as these are essential to any organization. It also requires a knowledge of markets and marketing, of products and product development, of customers, and of the processes of selling, buying, and anything else relevant to business performance.

### 7. Basic Strategies

Various strategies and approaches can be used to make change management successful. The four strategies are introduced here are based on different aspects of people and their behavior.

1. **Rational-empirical.** This approach is based on the understanding that people will follow their self-interest once it is revealed to them. In this instance, change is based on the communication of information and the proffering of incentives.

2. **Normative-re-educative.** The basis here is that people will adhere to cultural norms and values. Change, in this example, is based on redefining and reinterpreting existing norms and values, and developing commitments to new ones.

3. **Power-coercive.** People will generally do what they are told or can be made to do and so change is based on the exercise of authority and the imposition of sanctions.

4. **Environmental-adaptive.** People oppose loss and disruption but they adapt readily to new circumstances. In this example, change is based on building a new organization and gradually transferring people from the old organization to the new one.

Above all, it is recommended that the range of an initial change management project should be limited. This way, the organization can achieve partial success quickly. The change management process can be then kept going by continuously increasing its range and scope.

Strategies should be used flexibly and possibly in combination. No single change strategy is recommended above others and the approach adopted in any particular instance depends on a number of factors such as:

- **Degree of resistance.** Strong resistance argues for a coupling of power-coercive and environmental-adaptive strategies, while weak resistance or concurrence argues for a combination of rational-empirical and normative-re-educative strategies.

- **Target population.** Large populations argue for a mix of all the above strategies.
• **The stakes.** High stakes argue for a mix of all the above strategies.

• **The time frame.** Short time frames argue for a power-coercive strategy, while longer time frames argue for a mix of rational-empirical, normative-re-educative, and environmental-adaptive strategies.

• **Expertise.** Having adequate expertise available argues for some mix of the above strategies, while not having it available argues for reliance on the power-coercive strategy.

• **Dependency.** If the organization is highly dependent on its people for one reason or another, then management’s ability to command or demand may be limited. Conversely, if people are highly dependent upon the organization, their ability to oppose or resist may be limited.

### 8. Tips to Manage Change Management

Successful change management is more a matter of leadership ability than managerial skill. It is pretty much the same as managing anything of a turbulent, messy, or chaotic nature. Therefore, the first thing to do is to jump in. It is important to involve everyone inside the organization who is relevant or who has an interest in the change process, as it is impossible to do anything from the outside.

- A clear sense of mission or purpose is essential. The simpler the mission statement the better.
- Build a team. Managing change requires an intelligent team and an excellent team leader.
- Maintain a flat organizational structure and rely on minimal and informal reporting requirements.
- Pick people with relevant skills and high energy levels.
- Toss out the rulebook. Change calls for a configured response, not adherence to prefigured routines.
- Shift to an action-feedback model. Plan and act in short intervals.
- Set flexible priorities. Have the ability to drop what is being done in order to attend to something more important.
- Treat everything as a temporary measure. Do not ‘lock in’ until the last minute, and then insist on the right to change your mind.
- Ask for volunteers. Do not overlook volunteers and their abilities.
- Find a good ‘straw boss’ or team leader and stay out of his or her way.

Give team members whatever they ask for – except for undue and unnecessary authority. Generally only resources are sought. If a team asks for increased authority, it may be a signal of an impending power-based confrontation and could indicate trouble. It is important to understand the basis of the request before acting as it could be due to other reasons and it may highlight issues that need to be resolved as part of the change process.
Concentrate dispersed knowledge. Keep the communication barriers low, widely spaced, and easily hurdled.

Last but not least, acknowledge that the task of change management is to bring order to a messy situation, do not pretend that everything is already well-organized and disciplined.
Content Management

1. Introduction

To be able to provide information at any time, location, or method and to be able to do so cheaply and quickly is rapidly becoming the stated requirement of organizations around the world. Governments, as the largest holder of information are stepping up to the challenge of providing information and services online. Content management is regarded as a key enabling technology in moving governments online. It is an important driver in successful e-government initiatives.

2. What is Content Management

When information is given a usable form intended for a particular purpose, it becomes content. Content can be a legacy document, information in a friendly web format, or a commercial transaction. The value of content is based upon the combination of its primary usable form, along with its application, accessibility, usage, usefulness, brand recognition, and uniqueness. Content management is a process of collecting, managing, and publishing information and functionality to a set of target audiences.

- To collect content, an organization must set up a system that effectively captures the information and the functionality that the organization wants to deliver. In addition, the system must ensure that the content has been appropriately and consistently tagged to be part of the organization’s content scheme.

- To manage content, an organization must set up a system to store and organize information and functionality outside of any particular delivery channel. It is important to make sure that the stored and categorized content is easy to find and retrieve.

- To publish content, an organization must set up a system to design and deliver the right information and functionality in the ways that the organization’s audience expect and will respond to favorably. The publishing system has to manage a comprehensive web site and other publications that an organization needs to provide.

Content management systems are used to store and retrieve massive amounts of information. They are used to create information portals that serve as the backbone of knowledge management. Content management is a broad process of collecting, managing, and publishing information through whatever medium is needed.

3. Why Content Management Is Needed

A core function of many governments is the production, delivery, and archiving of information. Increasingly governments have applied technologies for managing their functions through online means, having realized that the Internet provides a great opportunity to improve service quality and information delivery. E-government is not only driven by the supply side of information which has an interest in the effective and efficient delivery of information, but also by the demand side, particularly
the expectation of the users concerning the usability and breadth of functionality.

Government agencies which want to manage and disseminate information and provide online government services will undoubtedly benefit from a solid content management system. A website that cannot provide reliable, accurate, and relevant information will bring lost profits and diminished reputation. Basically, there are three reasons for attaching importance to content management.

1. Content management gives substance to today’s notions of e-government. Content management is the way to make an e-government real and workable, as it can help constituents to reach the right information and transactions at the right time.

2. Content management is an antidote to today’s information frenzy. Contributors are putting more and more information onto websites in order to fulfill user’s expectations. Content management can organize and direct information as well as keep it under control.

3. Content management addresses the question of how to give particular value and substance to a piece of information. Content management systems create and manage information and tag them with the information that might be needed to identify their value.

The management and publishing of content through a website is a critical component of an e-government initiative. It is important that the content is correct and up to date, and it has to be seamlessly accessible through a number of different self-service modules. Content management acts as an enabler to e-government; it facilitates the assembly of content from multiple sources. In addition, it is flexible enough to support the wide range of applications and functionality characteristics of e-government initiatives.

4. **Key Requirements for Content Management**

The content management system should be flexible enough to manage content from small workgroup-level deployments as well as from organization scale implementations. The ability to quickly establish a functional environment with minimal maintenance effort is also critical. In addition, a content management system has to make information as accessible as possible so that citizens and employees can make informed decisions. These are the common requirements for content management. However, for e-government initiatives, the following key requirements may be also taken into consideration.

1. **Speed of deployment.** Government organizations need a solution that can be deployed quickly and is able to grow as the requirements grow. Due to the limitation of technical resources, a system that can be implemented without taxing existing resources is the key to e-government initiatives.

2. **Ability to publish materials and convert them from original formats.** A content management system used in e-government initiatives must be able to easily convert both paper and electronic content to a format that is readily accessible through the web. Moreover, the system should allow content owners to manage the source content and make updates over time, while automatically reflecting these updates in the ‘public’ version.

3. **Ability to automate the publishing process with templates, using familiar tools.** A system that provides a template-based approach streamlines the publishing process, by allowing pre-defined templates to be created and used by content authors. Authors can use familiar tools to create content and be confident that the results will look seamless when published on the website.
4. **The need for direct content contribution from a geographically dispersed workforce.** The system must be all-inclusive in terms of access for authors and users. Accessible to all functionalities through popular, platform-independent web browsers is critical.

5. **Support content expiration, archival and retrieval.** The system should provide the ability to archive content for later access in an organized, searchable, and knowledge-based format. It should be able to scale up to support large volumes of information that have been collected over time and provide facilities to dispose of content that is not frequently utilized or exceeds its retirement date.

6. **Must support a security model that gets the right content to the right people.** E-government usually needs systems that are flexible enough to support public websites as well as intranet deployments. Therefore, the content management system should support a dynamic security model that is flexible in supporting both private and public models without a huge administrative burden.

7. **Support a large-scale number of users, huge content repositories and a diversity of authors.** Government systems involve many users with varying technical expertise and large volumes of content. Therefore, a system should be scalable and robust in a high volume production environment.

8. **An open technology based on industry standards.** In order to save implementation fees, to increase the ease of integration with other systems, and to protect the investment in content management as needs and usage grow over time, the system should support industry standards and have open architectures and development environments.

9. **A solution that provides significant value for money.** A system that is affordable and does not require a large implementation is critical for its adoption across government organizations. Solutions that have this added value are of particular interest to e-government initiatives, as government organizations can ‘piggy back’ on existing implementations or customer developments.

**5. Action Plan for Content Management**

When government is moving towards online service, it is necessary to have an action plan to meet the requirements of managing the web content efficiently and generating new ideas for advanced services. Such an action plan may include the following items.

1. **Establish the goals and metrics for initiatives.** These goals and metrics can be used as a measurement of the progress and success of e-government initiatives. Some areas that need to be taken into consideration are

   (a) Increased efficiency for both ‘online’ and ‘offline’ activities. The proper content management process can help to manage and publish information on the website without technical intervention. Thus the users are able to collaborate efficiently with co-workers and manage information and documents securely and efficiently.

   (b) Decreased process time for publishing and delivering content. Content creation and delivery time can be used as another metric to evaluate the success of e-government initiatives. By using proper content management systems, critical information can be published as soon as it is created and approved through an automated workflow.
(c) Increased quantity of online services. By using a content management system, important content assets are organized in an open system and under control. The number of services offered online versus offline can be another indicator for measuring the success of e-government initiatives.

2. **Understand what services need to be deployed.** A logical and prioritized plan for the services that need to be deployed can help an organization to work on specific functionality for those high priority services while building the content management foundation. Content management will be a fundamental building block for the web initiative.

3. **Get users involved.** A content management system should be flexible enough to accommodate changes to both creation and delivery processes. It is better to involve users in the process early and implement the feedback they provide. Deployment of this feedback provides an opportunity to constantly refine the service offered.

4. **Get content ready.** The process of converting legacy content to web-ready formats is an often-underestimated portion of a content management deployment. It is better to start with a specific set of content and plan the conversion in a phased approach based on incremental value.

5. **Make sure there is a process to manage content.** Maintaining and managing content in an efficient manner is a greater challenge than getting content on to the website. Therefore, a plan to manage content from the beginning is vital, including document metadata tags that improve the quality of search functions. In addition, it is very important to establish processes that help users manage their own content.

6. **Look for a vendor that will support specific application needs.** The chosen vendor should have an open architecture and extensive experience with government implementations as these are important to the success of e-government initiatives.

**6. Managing Content with XML**

With its flexibility and simplicity, XML (eXtensible Markup Language) becomes a benchmark standard for publishing and managing content. XML was recommended by W3C (World Wide Web Consortium) in 1998. It supports many implementations on both the client and server sides and provides some database support, particularly from object oriented database vendors.

XML enables a content owner to handle the matrix of ownership that exists across the site. It also provides tremendous opportunities for creating scaleable campaigns and exciting content that could be maintained quickly, easily, and cost effectively. XML provides a natural way of establishing data standards across industries and markets without dictating look and feel. In addition, application data and traditional content can share a common vocabulary, and a common technology base.

XML provides excellent methods for content management. Data is held in easily managed text documents rather than in any number of disparate databases, so that tools are easy to develop and deploy. It cuts days from deployment times and reduces workloads, as it places the control of content back into the hands of the people who own it. In this case, users can make their own changes to content and see the effects for themselves, rather than going through endless revision processes.

Another property of XML is that it can easily handle special characters, for example, registered trademarks and trademark symbols. For special characters, only a separate style sheet is needed rather than an entirely separate set of all data documents.
When managing content, it is difficult to anticipate what users expect. Using XML will constrain users to an extent, and force content owners to adopt a more consistent approach. All similar data are in a similar format thus helping to keep data in a maintainable form.

Therefore, XML is a great way to store data in a way that an organization can digest and manage it. It becomes possible to model the entire content of a website by using a small set of XML vocabularies for different classes of documents that have clear ownership; which can be combined into pages published on the site through means of a devised content management system.

Furthermore, XML supports the maintenance of constantly changing data, such as news links to the home pages, or other special data that are created daily. It also supports longer documents, such as white papers or legal documents. Data maintenance has been made far easier than ever before by using XML technology.

Above all, XML technology makes it possible to manage content in a clear, simple, and consistent manner. It has had a significant impact on websites by helping to strike the right balance between creativity and ease of use.
Document Management

1. Introduction

Documents hold incredible power in government business environments and are undergoing a major evolution that will shake up government businesses and reform them into different entities. Therefore, the control and distribution of critical documents in a systematic fashion has become increasingly important, and similarly the need for reliable access to documents has become imperative.

2. What is Document Management?

A document is defined as a package of data structured for informational purposes. Documents have literally become unbound, no matter whether they are in paper-based entities or in digital components. A document is a collection of pointers and rules that can simultaneously engage a number of different information components and actions. It becomes a dynamic resource that can proactively route itself through an organization and brings procedural and information integrity to a business.

Document management is a technology and a discipline that traditionally augmented the capabilities of a computer’s file system. By enabling users to characterize their documents, which are usually stored in files, document management systems enable users to store, retrieve, and use their documents more easily and powerfully than they otherwise could within the file system.

Nowadays, document management includes additional valuable functionalities, which are

- Version tracking to check how a document evolves over time.
- Document sharing to check how a document is used and re-used in different business processes.
- Electronic review to allow users to add comments to a document without actually changing the document itself.
- Document security to refine access controls on different documents for different users.
- Publishing management to control the delivery of documents to different publishing process queues.
- Workflow integration to associate a document’s life-cycle with people, projects and schedules.

3. Why is Document Management Needed?

As documents rise in importance and become more pervasive, managing them becomes a crucial, organization-wide activity. There is no doubt that unplanned, unmanaged documents can cripple communications, deplete organizational resources, and perhaps most damaging of all, stunt organizational growth to the point where the organization fails to thrive. Therefore, proper document
management can help an organization to achieve unprecedented levels of control, insight, and competitive advantage.

Organizations are now being forced to examine their needs and goals and review the type and nature of the information they collect and to establish a procedure for document use. Document management provides fast access to the correct version of an organization’s document in order to meet the organizational development requirement of this information-rich environment.

Above all, document management can

- **Increase productivity.** Through web browser and client/server access, crucial business information is available instantly throughout the organization.
- **Reduce overhead costs.** By using electronic data storage and comprehensive archival capabilities, the costs associated with the overhead and legal issues of physically maintaining paper-based document are eliminated.
- **Access information uniformly.** In whatever form the document is archived, all critical organization information is accessible to the extended organizations through the Internet and portal application.
- **Manage all information.** All file types in logical groupings and indexes are combined and thus can be captured in a central electronic repository.
- **Streamline business processes.** Documents can be routed through complex business processes, reducing errors and saving time.
- **Access information quickly.** Vast databases are cross-referenced with automatic meta-tagging, so users can locate information within seconds.
- **View information clearly.** Documents are cleared and scanned, so there is no question about the accuracy of data.
- **Manage liability risks.** Document retention rules are applied at document creation, so litigation risks are reduced through definition of automated legal document retention rules.

4. **Document Storage**

Storing documents in digital format rather than on paper allows businesses to accommodate an effective and optimal flow of information. This provides a means for rapid finding, retrieving and sharing of all documents stored within an organization’s document system.

There are three primary methods of creating a digital document.

1. Scanning for paper files. Scanning a document can produce a picture image that can be stored in a computer.
2. Conversion for creating unalterable images of electronic documents. Converting documents is the process of transforming electronic word processor or spreadsheet information into a permanent image that can be stored in a computer.
3. Importation for creating modifiable versions of electronic documents. This is also known as
electronic document management. It is an alternative method of creating electronic files, such as audio and video files, that are stored in a computer in their native format and are modifiable.

Once brought into the system, a document has to be stored. There are many storage devices available for long-term document storage. Above all, documents must be stored in a non-proprietary format to ensure reliability in the future.

At present, there are five storage options as follows:

1. **Magnetic media (hard drives).** This device can be used to store a large number of documents, and can provide a fast response time. However, magnetic media contain moving paths, and data stored on them can be completely erased by mechanical failure.

2. **Magneto-optical storage (MO disk).** This device employs both magnetic and optical technology to obtain ultra-high data density. The chief limitation of MO disks is that they are slower than hard disk drives and are still subject to mechanical failure.

3. **Compact discs (CD).** On CDs digital information is encoded as a series of microscopic pits on the reflective surface of an aluminum disc. CDs offer a safe and reliable media that can provide a long-term storage option for images. Furthermore, CD-ROMs do not require specialized hardware or software to retrieve information. The primary drawback of this media is its limited storage capacity.

4. **Digital Video Disc or Digital Versatile Disc (DVD).** DVD is the next generation of optical disc storage technology. It is essentially a bigger and faster CD that can hold more information including video, as well as audio and computer data, by packing more data into the same physical space as a CD. It permits random access to any point on the disc. DVDs have unprecedented widespread support from all major electronics companies. The drawbacks of this media are its high cost and an ongoing battle with standards, as different manufacturers are using different formats for rewritable DVDs.

5. **On Write Once, Read Many (WORM).** Worm Data is permanent and can be read any number of times. This media format is not readily available and requires specialized hardware and software to operate. It is not strongly recommended due to the limited number of companies that provide materials and support for this technology.

## 5. **Document Retrieval**

One of the purposes of document management is to help users to easily find and retrieve the information they require. Several techniques are available.

- **Free-text search.** A document is retrieved by its particular subject. This technology assumes that users are familiar with a document's subject, and know precisely what they are looking for, as well as which words to use to best describe it. In reality, this technique is time-consuming and success in finding the document is not guaranteed.

- **Indexing terms.** Documents are retrieved by constructing and using queries made up of indexed terms. This enables users to formulate fairly sophisticated searches. The complex relationships between a set of control terms are defined, which improves the chances of finding the required documents.
• **Classification.** Documents are retrieved by browsing the hierarchy of categories. Documents are correctly classified within the search arena, which makes document retrieval reliable and accurate. The need for exhaustive searches is removed, and there is an instant shortcut to the required documents.

6. **Document Classification Methodology and Process**

Accurate and reliable classification is essential for consistently successful document retrieval. In order to make the best use of the information held in highly heterogeneous document sets, the hierarchy of classification terms must be easily navigable. A straightforward definition of classification terms facilitates document searches. The larger the document collection, the more important the classification becomes.

Generally speaking, there are two types of classification methodology:

1. **Clustering.** In this method documents are grouped according to various metrics, usually by word density. This may result in a number of small clusters that are not always obvious or useful.

2. **Taxonomy-based, rule-driven classification.** This requires definition of pre-set classifications and then the use of rules to classify documents; it gives a transparent, repeatable and flexible paradigm to aid navigation.

It is obvious that clustering methods are not suitable for large, complex document sets. The best way to categorize documents is under expertly designed classifications, which are arranged in a clear and sensible hierarchy.

When classifying documents, firstly, there is a need for a general level of knowledge about the classifications and the subjects which are going to be used. Automated tools must have knowledge about the subjects that are going to be assigned to documents. This knowledge is essential to improve the quality of the results of the classification process.

Secondly, there is a need for detailed classification knowledge. Classification knowledge is a compound of words and phrases that are known to be associated with a particular subject area. Knowledge about the relative significance of these words and phrases is essential to the success of classifying documents. A classification decision relies on subtle observation, understanding, and assessment of the evidence available in the text. Therefore, there must be sufficient evidence to justify the decision.

Lastly, there is a need to understand that some documents will never be classified correctly under any existing term or framework. There are gaps and limitations in any taxonomy of classification terms, so a ‘probably’ right result will be the best answer that can be expected from the best classification tools. Therefore, classification tools should be designed to arrive at decisions which give probabilistic results expressing sufficient confidence rather than absolute confidence.

7. **Document Management System**

Government agencies deal with numerous documents every day and these documents have become the primary information resources of an agency. How to effectively manage these documents and make them accessible and retrievable has become a major challenge to managers as they strive to make the agency operate and function well.
A modern document management system consists of the storing, categorizing, and retrieval of documents, spreadsheets, graphs, and imaged (scanned) documents through electronic means. Each document will be assigned an index-card-like record that holds information such as the author, document description, creation date, and type of application used. Such documents usually are designed for archiving on less expensive tape or optical disk where they remain available for future access if necessary.

Modern electronic documents can contain multimedia information, including graphics, audio clips, and video clips and they are called compound documents. With the help of document management systems, physical documents may be scanned, indexed, and stored on computers for quick access. Imaged and archived documents can be retrieved in a matter of seconds. Optical character recognition is used to ‘read’ documents and to turn them into computer text files. Once stored, the document can be duplicated indefinitely. In addition, parts of the document can be cut and pasted into other documents.

A document management system is becoming essential as network users begin to take advantage of these technologies. A document management system can assist an agency to do the following:

- Manage documents that are distributed and stored in repositories throughout an agency.
- Provide services such as storing, tracking, versioning, indexing, and searching for documents.
- Manage document revisions and ‘audit trials’ to track where a document has been.
- Make information available both inside and outside the agency.
- Make it easier to access any kind of document over government computer networks and the Internet.
- Perform document imaging and forms processing.
- Provide workflow and groupware technologies for transaction-oriented and collaborative document management.

Therefore, agencies can, by means of document management systems, electronically manage all types of documents through their entire life cycle, regardless of their format. The process includes intake and production of paper-based, electronic, or faxed documents, as well as document tracking, archival, and retrieval. The system should integrate document management, imaging, and workflow processes into a single system. For example, a paper document can be scanned and integrated with e-mail, image, and text documents. In other words, the system should be able to be packaged and equipped with desktop and work group scanners for converting paper documents into digital files that may then be edited, stored, forwarded, and retrieved by multiple users over the network in the agency.

8. Workflow Management

The purpose of workflow management is to automate document procedures in an organization by replacing paper-based systems with an electronic based one. A network provides the routing system that moves documents to and from storage, and distributes them among users who need to view and make changes to the documents or sign the documents and validate their authenticity. Workflow management encourages workgroup collaboration by automating processes and eliminating footwork.
Editing and publishing is a typical example of a collaborative environment that can benefit from workflow management. In many government agencies, almost all the divisions and units are dealing with document editing and publishing. In an editorial services division of a parliament, for example, documents are transferred, in stages, from reporters through editors to production. Many people, including reporters, editors, members of the parliament, chief editors, etc. are involved in producing one document. By using the existing network and its resources, the entire process of document production can be automatically managed and the completed work can be stored in the servers of the system and eventually printed.

The key features of a workflow management system include

- Documents contain routing information that serves to distribute the document to predefined users or devices.
- Documents can have simultaneous access.
- A document is viewed as ‘under construction’ until it exits the workflow process. Authorized users sign off at various stages, locking parts of the entire document from further editing.
- The system software has a filing system as well as a queuing and workflow manager that keep the system running.

From a management point of view, a workflow system can help heads of divisions to track the flow of information and to better manage that flow. A workflow management system can eliminate many time-consuming and often expensive activities such as meetings, phone calls, and express mail deliveries. Workflow management also allows users to view large image files, graphics, sound, and even video. Therefore, it can help government agencies to manage their tapes, photos, and videos; something which may become very necessary in the near future.

9. Access Control

People are able to search for information through the Internet from different locations. This has made it necessary for organizations to maintain an appropriate level of access for different documents, in order to ensure their confidentiality and integrity. Therefore, a document management system should have two fundamental features:

- **Broad availability.** A broad level of access saves limited financial resources, intellectual capital and network bandwidth. To provide broad availability and access flexibility, document management systems must meet the requirements of offices with diverse needs and possibly in diverse locations. This is frequently done through CDs, notebook computers, or e-mailing of documents. Browser-based document access removes the limitations of location and computer platform. In addition, sharing documents through the Internet or an intranet allows system administrators to deploy a document management system across their entire network or even to the public.

- **Comprehensive security.** A comprehensive security system must allow the system administrator to control what folders and documents users can see, and what actions they can perform on those documents. A good access system will make a document available to every authorized person, whether in an office, at a remote location, or over the Web, all without compromising system security.
Storage Management

1. Introduction

Organizations are facing the challenge of efficiently managing the extraordinary amount of business data generated by electronic applications and transactions. The demand for storage capacity is driven by this information influx. In order to maintain competitiveness in this highly dynamic business world, an organization has to keep up with demands for storage growth.

2. What is Storage Management?

Storage is defined as the capacity of a device to hold and retain data. Backup and recovery are the main activities of storage management. A backup is a copy of electronic data used as a means of recovery should the data become lost, corrupted, or compromised.

Storage management expands beyond backup to include all the functional areas of systems management and is starting to look increasingly like systems and network management. However, storage management retains some unique requirements and characteristics.

3. Recovery Types

Organizations are placing greater demands on storage management, specifically in terms of enterprise backup and recovery. Backup will remain prominent in storage expenditures. Organizational backup is defined as the requirement for central support through backup and recovery automation products. These products must satisfy requirements for backup/recovery performance, availability, operational automation, and service/support.

The focus of backup has shifted to recovery, as recovery is a key element of any storage management implementation. It is data availability failures that require recovery in any organization. There are four types of data availability failures:

1. Hardware failures in the disk driver/server environment.
2. Disasters.
3. File/directory deletion.

The problems caused by these failure types can be addressed by unique recovery solutions as follows:

- **Hardware failures** can be addressed by using a redundant array of independent disk (RAID) techniques within a disk array. The vast majority of disk hardware failures can be mitigated by RAID and redundant components. However, RAID does not address power or connectivity failures within a frame or chassis, and any data changes made between the
backup and the disk failure would be lost.

- **Disaster** can be addressed in a number of different ways. Remote replication techniques can ensure zero data loss in the case of disasters, but the cost of a second remote data center is high. Remote replication in combination with an application environment at the recovery site is an alternative. This can provide fast recovery times, as, upon failure of the main site, the remote site is activated and acts as the primary site. Offsite vaulted backup tapes are used as a primary recovery mechanism. However, data added or modified between the last backup and the disaster is lost in the recovery from tape.

- **File/directory deletion** can be addressed by Snapshot technology. The majority of this type of failure is caused by user or operator error. Replication technology does not help in this case because deleting a file will also delete it from a locally or remotely replicated disk or volume. A point-in-time copy of a disk or volume may contain the deleted file. However, snapshot technologies are often used as the basis for backup but they are not yet ubiquitous.

- **Application/database corruption** can be addressed by transaction-level recovery tools. More traditional database recovery functions use the database log to roll back and roll forward. This type of failure is often not immediately detected, as it is often caused by a bad transaction or an application error that has been introduced into a production system. A backup or a snapshot is used as the basis for log-oriented roll-back or roll-forward techniques.

Organizations should have developed recovery scenarios, processes, and requirements against the four different fundamental failure types, and tailored their data availability requirements and budgets to accommodate the recovery requirements of each of the four failure types.

### 4. Storage Management Systems

Network Attached Storage (NAS) and Storage Area Network (SAN) are technologies that enable organizations to realize the benefits of networked access and delivery of information assets.

In NAS, a storage device is directly connected to a network that presents industry standard network file system interfaces. NAS devices provide a file level interface to the outside, and use a block level interface to either tightly coupled or loosely couple storage sub-systems. The file system resides in the NAS appliance.

SAN is a dedicated storage network designed specifically to connect storage, backup devices, and servers. SAN may be consolidated into a single box or cabinet, or span a large number of systems and geographic locations. SAN is connected behind the servers and presents a block level interface to the outside. The file system resides in the server.

The key difference between SAN and NAS is the access method. SAN systems have become a popular method of providing storage consolidation due to their use of Fiber Channel. SAN systems present block interfaces while NAS systems present file interfaces. NAS systems are typically more efficient when serving files while database engines and large block I/O operations typically utilize block interfaces.

Other components of network storage may include

- **Direct attached storage (DAS)**, a traditional method of locally attaching storage to servers
in which the communication path between the server and storage is dedicated. These systems may be just disk drivers, a RAID sub-system, or some other storage device.

- **Network attached storage head-end (NAS)**, an appliance that separates the NAS function from the storage subsystem. Some appliances use tight integration between the NAS appliance file system and the RAID or disk system which limits their use in open storage networking.

- **Block access system**, a storage system or sub-system that presents a block interface to data.

- **File and/or record access system**, a storage system or sub-system that presents a file or record level interface to data.

5. **Similarities and Differences between Storage and System Management**

Storage management systems are looking more like systems and network management. As far as topology mapping is concerned, the SAN management tools are focused on discovery, topology mapping, and status monitoring and these are the same functions provided for TCP/IP networks. The performance and availability are much the same for both systems when it comes to collecting and storing information and making reports about performance and availability. Capacity analysis and chargeback can be accomplished with different data collectors, but with the same accounting and reporting facilities for both systems.

However, storage management differs from systems or network management in some fundamental and important ways.

Storage management is more active and proactive than typical network system management. One unique and basic attribute of storage management is the fundamental need for active management. Backup is proactive fault management performed by actively preparing for a potential recovery.

Performance management for both systems is similar in concept, but the approaches are radically different. System management performance analysis is typically effective when using data that is collected and summarized over a period of seconds or minutes. Storage performance monitoring requires agent technology, operating system, file system, and disk array instrumentation that is well beyond the generic storage analysis capabilities of general-purpose systems management products.

The primary issue of storage availability management is not fault discovery, but integration with other fault data to discover the root cause.

In addition, most systems and network management is done in-band to agents that reside directly on the server or network device. Most storage management is done out-of-band to a console or agent that resides in the disk array or SAN switch. NAS storage is often managed in-band because the TCP/IP stack is already there as part of the in-band communications.
6. **Basic Requirement for Storage Networks**

As part of an organization's IT infrastructure, a storage network is a proven solution that provides superior scalability, higher availability, and simplified management. It plays an ever more vital role within the overall IT infrastructure of an organization. With such a prominent role, a storage network has to be

- **A proven solution.** It should be tested in a wide range of industries and application environments, and supported by a variety of server and storage vendors. It must also fulfill the performance requirements expected of server-to-storage connections.

- **Scalable.** It should be able to scale independently of storage and server capacity and maintain accessibility of data at the same time. It must also provide excellent configuration flexibility and extended distance connectivity.

- **Low management cost.** It should be manageable with a minimum of direct management or, ideally, be manageable by existing tools that manage applications, storage, or servers.

- **Highly available.** It should be continuously available with limited downtime and built-in redundancy.

- **Secure.** It should be secure, with reliable authentication devices and specific access control mechanisms.

- **Heterogeneous.** It should have interoperability and be designed on the basis of open industry standards to support the widest range of devices.

- **Accommodative.** It should be able to grow and adapt to new requirements and technologies. It must be controlled by a set of management services that can be extended to accommodate new storage protocols.

7. **Ten Steps of Backup/Recovery Practices**

The majority of management disciplines associated with storage management is oriented toward backup and recovery. To meet this demand, an organization must take the following ten steps to provide a high level of recovery services at a reasonable cost.

1. **Standardize backup products.** This makes centralized monitoring and administration of backup services possible, and provides operational economies of scale. In addition, it limits the amount of training needed for specialized tools and also limits the time spent managing vendors.

2. **Focus on recovery.** Recovery solutions that go beyond traditional recovery from tape should be considered and concentrated on the recovery aspects of backup.

3. **Build a dedicated storage management organization.** This helps to meet service level agreements (SLAs) and document procedures. It supports the integration of storage management into business and operational processes and lowers the failure rate for backup and recovery.

4. **Define recovery SLAs.** Including the backup and recovery time constraints and the data
currency and data retention required in order to determine the design of backup deployment. Recovery SLAs should drive backup deployment.

5. **Develop backup process deployment standards.** The backup process should be based on recovery requirements, backup data size (by server), network bandwidth constraints, and application recovery time requirements. The deployment should involve a combination of centralized backup servers and local backup service deployment.

6. **Document procedures for backup operations.** Distinct backup processes for major system elements are needed for an optimized process. Documents should be reviewed and updated whenever there are problems, infrastructure updates, or failures that necessitate procedural backup changes.

7. **Centralize backup process for monitoring and administration.** A centralized backup process for monitoring and controlling backup operations is required. The backup activity logs daily for errors and a system that assigns responsibility for resolving them is needed.

8. **Document procedures for recovery operations.** The recovery types determine the recovery procedures, and a system administrator may define recovery steps or verify the integrity of a database or information storage after recovery. Documents should be reviewed and updated whenever there are problems, infrastructure updates, or failures that necessitate procedural recovery changes.

9. **Integrate with change control and application development cycles.** Changes to applications may affect the integrity of the backup/recovery process. Therefore, the change control process should interface with application development areas to collect information about backup/recovery requirements and service levels prior to production deployment.

10. **Test recovery.** Testing the recovery process is the only way to ensure the possibility of recovery. Periodic testing of system and application level recovery capabilities is required. The multiple levels of testing may include single file, directory, application data, database or information store, operating system, and full system recovery.

These 10 steps of a recovery/backup process can help organizations to lower the total costs of their backup and storage system and achieve a high quality of recovery service.
Knowledge Management

1. Introduction

Organizations are increasingly relying on their intellectual assets rather than the tangible assets they manage. Knowledge management solutions are becoming the key to building and sustaining intellectual capital assets and using them to create economic value. Knowledge management solutions enable individuals, teams, and communities to perform much better in creating, capturing, sharing, and harnessing knowledge.

2. What is Knowledge Management?

There is a distinction between data, information and knowledge. Data are a property of things and can be observed directly. Information is the accumulation of data into a higher level cluster that holds meaning and significance. Filtered through the perceptions and thoughts (cognition) of a person information stimulates a rich variety of action and activity.

Knowledge is extracted from data and builds upon information. It falls into two distinct forms:

- **Explicit knowledge**, which consists of forms of information, expertise, or experience that can be articulated in detail, archived, codified, rendered persistent, and shared with the help of IT. Explicit knowledge can take the form of a database, document, drawing, formula, patent, video, or presentation.

- **Tacit knowledge**, or the know-how contained in people’s heads. Tacit knowledge is a common, unarticulated system of values, vision, purpose, and behaviors that directs an organization’s activities. It is experiential. Identifying tacit knowledge is a major hurdle for most organizations. The challenge inherent in tacit knowledge is how to recognize, generate, share, and manage it.

Tacit knowledge can only be inferred through the actions of people, it cannot be directly observed. Such knowledge is a property of people and predisposes them to act in particular ways in particular circumstances.

Knowledge management is systematic management. It is a process of compiling, using and reusing information, explicit knowledge, experience, and expertise to achieve a special business benefit, goal, or objective that makes the organization more competitive and profitable.

An organization generates value from its intellectual and knowledge–based assets through this process. Knowledge management is an enabler of innovation and learning.

Knowledge management solutions have to bridge the gap between explicit and tacit knowledge. These solutions employ content technologies that support the capture and management of explicit information as well as collaboration technologies that enable individuals and communities to create, share, and socialize information to meet specific business objectives.
3. The Importance of Knowledge Management

In today’s information-driven economy, organizations derive the most value from their intellectual rather than their physical assets. Knowledge management helps to maintain the knowledge that must be shared if it is to serve as the foundation for collaboration. Furthermore, knowledge management helps an organization to:

- **Foster innovation.** Knowledge management provides an infrastructure for electronic and social networking to develop new products or services; it fosters and provides access to rich pools of ideas so others can capitalize on them.

- **Foster collaboration.** Knowledge management increases collaboration opportunities; it enriches the exchange of tacit and explicit knowledge between people; and it encourages the free flow of ideas.

- **Encourage and use learning.** Knowledge management facilitates and accelerates learning; it creates opportunities for individuals and groups to put new knowledge to use; it leverages organizational knowledge and brings the right information to the right people in an understandable context that addresses new challenges; it values individual learning by rewarding it and leveraging it to the organization level.

- **Foster social capital.** Knowledge management increases the transfer of individual knowledge to the organization; it fosters exchange across organizational boundaries, time and space; and it links people who have the requisite tacit and explicit knowledge with those who need it to do their jobs.

- **Attract and retain human capital.** Knowledge management enhances employee retention rates by recognizing the value of an employee’s knowledge and rewarding her/him for it; it captures and leverages what people know – their ‘know how’ and ‘know what’; it promotes career growth.

- **Create and use structural capital.** Knowledge management converts intellectual capital to structural capital; and it focuses strategic thinking on capitalizing on knowledge rather than focusing on the budget.

- **Enable e-government.** Knowledge management provides an IT-enabled information base to enable citizens and customers to access information and services they need; it establishes a network of knowledgeable government employees who can add value to citizens’ or customers’ requests.

- **Increase productivity.** Knowledge management streamlines operations and reduces costs, risks, learning curves and start-up time by eliminating redundant or unnecessary processes; it contributes to bottom line/mission goals.

- **Share best practices/processes.** Knowledge management shares best practices across the organization; it learns from failed efforts; it provides a platform for knowledge re-use and innovation; it establishes benchmarks for internal and external performance of individuals and teams; and it assists new employees in acclimating to the organization culture quickly.

- **Provide leadership and decision-making.** Knowledge management provides the right information in a context that aids decision-making; it integrates new knowledge into decision processes by sharing and collaborating with players and stakeholders in decision-
making processes; and it uses information and knowledge to align organizational actions with missions and visions.

- **Increase customer satisfaction.** Knowledge management improves customer service by streamlining response times; it focuses on the knowledge of customer needs to drive an organization’s efforts; and it improves customer outcomes and experiences with services rendered.

- **Create competitive advantage/market differentiation.** Knowledge management helps to achieve knowledge superiority; as a business proposition, product or service, it changes the value proposition from delivering goods and services to delivering knowledge and expertise about those goods and services; and it focuses collective organizational intellect on customer needs to meet business/mission goals.

4. **Challenges Facing Knowledge Management**

In the creation of innovative products and services, some organizations may still lack the ability to plan effectively and strategically, access the operation, and are unable to implement the services and systems required for business successfully. These may become a hurdle to knowledge management implementation. Other challenges include

- **Getting employees on board.** A culture that recognizes tacit knowledge and encourages employees to share is critical to knowledge management. Employees are encouraged to surrender their knowledge and experience – the very traits that make them valuable as individuals. Furthermore, employees who do participate may be apprised on the basis of the quality or relevance of the information they contribute. Knowledge management programmes have to reassure participants in these respects.

- **Allowing technology to dictate knowledge management.** Knowledge management is not a technology-based concept. Therefore, an organization should not be duped into establishing a knowledge management programme solely on the basis of promises made by any particular collaborative tool. Technology can support knowledge management, but it is not the starting point of a knowledge management programme.

- **Not having a specific business goal.** A knowledge management programme should incorporate a specific business goal.

- **Keeping knowledge management updated.** The content in a knowledge management programme needs to be constantly updated, amended, or deleted. Moreover, the relevance of knowledge at any given time changes, as do the skills of employees. Therefore, a knowledge management programme is not static.

- **Distilling information into knowledge.** Organizations need to be on the lookout for information overload. The point of a knowledge management programme is to identify and disseminate knowledge gems from a sea of information.

5. **Road Map to Knowledge Management**

A strategic plan can act as a navigator for a successful of knowledge management implementation. It can help an organization get started down the right path and stay on course while roadblocks spring up in the way. The steps essential to the achievement of true knowledge management implementation
can be set out under the following five stages:

5.1 Stage 1: Get Started

The first thing that needs to be done as an organization embarks on the journey of knowledge management implementation is to create a clear picture of the tangible benefits of knowledge management in relation to the organizational goals. Simple definitions and simple language should be used to explore real problems, opportunities, and the potential value that knowledge management addresses.

Next, identify others who can, will, or should support knowledge management. In particular, identify the motivating factor most likely to influence others in the organization to participate in and support knowledge management initiatives.

Then, look for windows of opportunity to introduce the benefits of knowledge management. Find where knowledge management will be most valued by talking to people inside the organization involved with strategic initiatives and internal consulting groups and identify people likely to have an interest in knowledge management.

Finally, capitalize on the Internet and enlist the IT department to provide tools and put forward a balanced view of knowledge management. The IT department can be a catalyst for the identification, development, and use of emerging knowledge management support technologies.

Roadblocks at this stage can stem from ignoring the culture or history of an organization by not addressing issues that might hinder knowledge management; attempting to sell an organization-wide approach without first building evidence; and asking for a large budget before creating a compelling value proposition.

5.2 Stage 2: Develop a Strategy

The formulation of a knowledge management strategy that fits the business model is often the turning point of the implementation process. During this process business opportunities may be identified and related pilot initiatives put in place. A task force may take charge of these activities on behalf of the organization.

It is essential to form the task force first. The priority is to identify opportunities for pilots and set the standards for methods to be used across all initiatives.

The next step is to select the pilots or identify current initiatives that could work as pilots. This can be achieved by either selecting new strategic pilots or adopting current grassroots efforts already under way. Selecting pilot sponsors with the resources to help the initiative along is also necessary.

The last step of this stage is to find the resources to support the pilot. Resources such as skilled staff members, who can facilitate the initiative and who are authorized by management to focus their time on it, or IT applications that might need to be acquired, created, or modified.

5.3 Stage 3: Design and Launch Knowledge Management Initiatives

At this stage, knowledge management begins to take definite form. This is the time to harness the momentum from the first two stages and to focus on details.

Funding the pilots marks the beginning of this stage. The formation of a steering committee or cross-unit task force is recommended for knowledge management initiatives to provide oversight and to
reallocate organizational resources, such as money and time.

The second step is to develop methodologies that can be replicated. It is important to form an active community to contribute to the effort and establish a process for screening, filtering, and validating shared knowledge from the community before presenting it as organizational knowledge.

Moreover, it is important to capture the lessons learned from the process. To complete this most crucial last step, the oversight group must discuss lessons learned at regular meetings and provide a common space for sharing the results.

5.4 Stage 4: Expand and Support the Initiatives

At this stage, knowledge management initiatives can be escalated rapidly. Their growth will be highly visible. Being given the green light to expand brings the added pressure of meeting formal business evaluations and providing justification in business terms. However, knowledge management at this point is well on its way to being considered a necessary organizational competency.

Developing an expansion strategy is the first thing that needs to be done at this stage. This can be achieved either by choosing to apply the pilot selection criteria to programmes in other departments step by step, or by developing an all-at-once strategy to implement knowledge management universally. Appropriate resources, necessary technology, and available user support is necessary in either approach.

Communicating and marketing the strategy are the next things to be done. It is necessary to publicize knowledge management initiatives throughout the organization so as to get everyone involved in the process.

Managing the growth is the last but the most important thing to be actioned at this stage. Controlling the confusion from the explosion of knowledge management initiatives that normally happens at this stage is critical to the success of the whole process.

5.5 Stage 5: Institutionalize Knowledge Management

This is a destination and also a new beginning for knowledge management. Here, the organization is beginning to understand that knowledge management is a business strategy, not just a database, and needs to be an integral part of the organization’s business model. Knowledge management at this point becomes accepted as a necessary organizational competency with unlimited potential to benefit every unit of the organization.

The first step of this stage is to embed knowledge management in the business model. It is necessary to obtain support from senior management for this.

The next step is to realign the organization's structure and budget. The organization should reorganize budget and departmental responsibilities so as to accommodate the wide deployment of knowledge management as a business strategy. The organizational structure will, to some extent, naturally evolve to better fit this new way of working.

The third thing that needs to be done is to monitor the health of knowledge management. Employing an external evaluation panel, conducting internal maturity evaluations, or including knowledge management feedback on employee surveys can take the pulse of knowledge management initiatives regularly.
The next task is to align performance evaluation and rewards with the knowledge management strategy. Reviewing knowledge management performance sends a dramatic message about its role because performance appraisals are the basis for promotion and pay.

The penultimate steps are to introduce local controls as a balancing feature within the organization-wide knowledge management framework and to link organization-wide business goals to knowledge management activities so as to provide the necessary coherence and consistency. Individual groups should be allowed to develop knowledge management resources that meet their specific needs. However, knowledge management policy should always be driven by business needs.

The last thing that needs to be done at this stage is to make arrangements to continue the journey. While the organization is becoming a true knowledge-sharing organization at this stage, demand for knowledge processes will continue to increase, as they will save time and money. Maintaining support from the senior leadership to help the organization in keeping pace with this demand is necessary.

By addressing and completing the key activities of each of the five stages, an organization will maintain a sound footing throughout the entire knowledge management implementation process.
1. Introduction

Information is an integral part of doing business in any government department or agency. All of the services that the government provides to citizens, to businesses, and to internal clients are based on information. Government has a wealth of information to support all aspects of the programmes and services that are, accessed by the public. Therefore, it is important to ensure the free flow of information between the government, citizens, and businesses. Managing information in a proper way is fundamental to most government activities.

2. The Functions and Elements

A framework for the management of information (FMI) in government can provide integrated, authoritative, and practical guidance for managing information by putting forward standards and guidelines. Such guidance will reflect information law and policy requirements as well as knowledge and practice, for which there is widespread consensus in terms of value and usefulness. It will also contain new ideas to meet the evolving needs of electronic service delivery. Therefore, FMI serves to provide the ‘how to’ type of practical guidance. It is also a ‘living document’ that reflects the changing environment surrounding information flows.

The Framework for the Management of Information of the Government of Canada (Figure 1.1) is structured into three elements. They are

- The foundation which provides an overview of information management and establishes information management vision, goals, and principles; it also describes stakeholder perspectives and highlights legislative and policy requirements.

- Management of information guides is oriented to the needs of specific roles in information management; they describe roles and responsibilities and provide a coordinated view and quick access to the standards and guidelines that are relevant to a particular audience or role.

- Standards and guidelines themselves provide guidance on specific elements of information management, such as planning for information needs, retention requirements, categorization of information methods, and privacy considerations.
In order to improve citizen access and client satisfaction, the FMI focuses on citizens’ information needs, interests, and rights within the delivery of government programmes and services. It provides a single source of guidance on information management during its entire life cycle (Figure 1.2) as well as information about best practices with reference to online access to government information and services. It also facilitates the adoption of common management approaches to the delivery of information services in government departments and agencies.

The FMI fosters an environment for the responsible use of information while ensuring legitimate precautions are taken to maintain public trust. In addition, it sets the criteria for quality of information and information audits, supports the goals of accountability and transparency in all functions in the government, and ensures the integrity of information that is used in the analysis of programmes and services provided to the citizens and businesses.
3. **Vision, Goals and Objectives for Information Management**

Implementing an FMI is a long-term commitment. It is vital to have a clear vision, goals, and objectives to support day-to-day decision-making and to promote behavior consistent with common values.

The vision should identify the desired future for the government in its management of information. Achieving the vision is a long-term undertaking requiring commitment and co-operation by all persons working in the government departments and agencies.

The goals and objectives of information management provide a broad statement of desired outcomes in support of the vision. In general, the goals are to enable informed decision-making, to support transparency and accountability in the government, and to ensure access to information in accordance with legislation and policies about privacy and confidentiality.

The objectives are threefold:

1. To ensure the quality of information available in the government; to ensure that information is regarded as a valued strategic business resource that complies with existing legislation, regulations and policies.

2. To ensure that everyone working with the government understands their responsibility and knows that their performance will be appraised on the basis of their management of the information they create, receive, acquire, use, dispose of, or preserve.

3. To ensure the general application of the principles and practices agreed for the management of information and those that apply throughout its lifecycle.

The Canada FMI supports the government’s governance, improves programme and service results and supports workforce productivity. It also strengthens accountability by providing guidance on information management and enhances stewardship by strengthening the capacity of public services to protect and add value to information in the custody of the government.

4. **Principles for Information Management**

The principles for information management in government provide concrete values and beliefs to guide behavior in achieving the vision. The principles include but are not limited to:

1. Recognition that information is an integral part of doing business in government departments and agencies, and is required to support all aspects of government activities.

2. Information is a strategic, government-wide, business resource that is subject to legal and policy requirements.

3. Information is under the custodianship of government, and is accessible to the public, subject to legal and policy requirements.

4. Information of high quality is essential for the government.

5. Managing information is the responsibility of everyone working for the government.
5. **Legislation, Regulations and Policies**

Legislation, regulations, and policies provide a legislative basis and statutory direction for information management in government. They should be used as references to assist with planning and in designing checklists to ensure all information management requirements have been considered. In delivering programmes and services, government departments and agencies must ensure they respect government-wide information laws and policies as well as information related legislation and policies specific to their mandate. New legislation and changes of existing legislation should be taken into consideration when responding to citizens’ or businesses’ needs and or to a new opportunity or threat.

However, regulations and policies vary from country to country. They may include or address:

- **Access to information**, to provide the right of access to information in government departments and agencies, and to ensure effective and consistent regulations on a government-wide basis.
- **Copyright**, to protect ownership and the corresponding rights related to any material form, and to ensure that the ownership rights, associated with works subject to copyright, are fully respected in all media applications.
- **Personal information protection**, to limit the collection and use of personal information, and to ensure that personal information under the control of the government is used only for legitimate purposes.
- **Privacy**, to protect the privacy of individuals with respect to personal information held by a government institution and to provide individuals with a right of access to that information.
- **Electronic documents**, to provide for the use of electronic alternatives in the recording or communication of information or transactions, to allow the use of electronic signature to authenticate business transactions and to provide evidence in legal proceedings.
- **Security**, to protect the information held by a government institution from disclosure to an unauthorized person, and to ensure that appropriate safeguards for all sensitive information and assets of the government are in place.

6. **Information Governance and Accountability**

Information enables and supports the delivery of government programmes and services. It underpins the governance processes that ensure that the government serves the needs of citizens and businesses in an open, transparent, and responsible fashion; governance processes that also ensure that it is held accountable for delivering expected results.

All government institutions are accountable for managing information in their custody and for the effective use of institution and government-wide information. All persons working for the government are accountable for due diligence, quality results, efficiency of effort, and obedience to information policies and legislation related to their responsibilities.

However, government institutions must work in partnership with each other, with other government levels and jurisdictions, and with non-government organizations. Institutions must participate in defining and operating a common information management framework that provides authoritative, comprehensive, and integrated guidance for information management across the government of the country.
7. Stakeholder Perspectives

Stakeholders are individuals, groups, or organizations that have an interest or share in an undertaking or relationship and its outcome. They may be affected by it, impact or influence it, and in some way be accountable for it.

Taking a systematic, holistic approach to identifying and prioritizing stakeholder perspectives will assist government to deliver programmes and services that fulfill individual client needs, respect operational constraints, and preserve the interests of all people in a country. It is also an important factor in affecting the efficient and effective delivery of programmes and services.

Government is required to recognize, balance, and customize the needs and interests of all stakeholder groups which includes consideration and identification of all potential stakeholders in service delivery. A clear stakeholder perspectives map can help government to understand both broad and granular stakeholder perspectives. Thus stakeholder information rights can be taken into account at each stage of management activities.

Stakeholders should be made aware of their responsibilities for providing and using information, whether it is a client applying for a government service or a government employee providing internal information. Input and feedback from stakeholders provides valuable information to assist with determining stakeholder needs and in measuring their satisfaction.

8. Information Management Guides

There are three types of information management guides, which are targeted at particular audiences or special management activities. They are

1. Information management guides for service delivery. These describe management activities involved in the whole lifecycle of information. The scope includes roles and responsibilities, methods of information management, and the criteria, checklists, cases, examples, etc., that enable service delivery.

2. Information management guides for office activities. These describe responsibilities and obligations, practical approaches, criteria, checklists, examples, etc. to help manage information in government. This can be used as a handbook for all people working for government.

3. Information management services guides. These provide guidance on approaches and practices in support of information management services.

The following addresses additional services and activities.

- Archival management describes the processes used to appraise and determine if records are valuable.
- ATIP services management describes the processes that ensure access to government information in a proper way that is consistent with public interest and personal privacy.
- Data modeling describes processes used to manage data models and data standards, and used to liaise with business transformation and technology groups.
• Document/records management describes the processes used for managing information activities, (e.g., analysis, storage, identification of information value, and design of records management system).

• Library management describes the processes used for managing information in a government library, (e.g. acquisition of books and other publications, interchange agreements, customer service evaluation, and library systems).

• Information management discovery tools describe the processes used for information management tools that assist in information discovery, (e.g., directories, categorization tools, and search engines).

• Information management systems describe the processes used for the overall administration of information systems.

• Portal management describes the processes used for the management of primary portals together with the tools and techniques necessary for government-wide implementation.

• Web and other publications management describes the processes used for managing websites, (e.g. content review and approval); managing linkages between government and private sector websites; and archiving information.

• Other guides for the management of IM tools and services describe the processes used to manage other IM services/systems/tools such as correspondence, forms design, mail services, etc.

9. FMI Standards and Guidelines

FMI Standards and Guidelines are categorized into the following domains which complement each other. They are:

• Management related standards and guidelines. These provide guidance on integrating management requirements and functions with the aim to manage information as a strategic business resource. This is to ensure that a strong governance and accountability framework is in place for managing information, and information management considerations are included in all management functions.

• Information life cycle standards and guidelines. These address considerations and requirements at each stage of the information life cycle. Specific requirements will be defined by the nature and the uses of information. The major stages in the life of information usually follow the need to plan, collect, create, receive, capture, organize, use and disseminate, maintain and preserve, and ultimately dispose of it. The basic rules and considerations to guide information management should be identified at each stage.

• Common legal and policy requirements standards and guidelines. Common legal and policy requirements that should be considered and obliged at all stages of the information lifecycle. This includes access to information, privacy and confidentiality, intellectual property, security, liability, official languages (where applicable), and communications. All these elements can protect and safeguard information used in government activities.