AGENCIES

ELECTRONIC RECORDS MANAGEMENT AND ARCHIVES MANAGEMENT POLICY

Guidelines on Electronic Records Management

NATIONAL ARCHIVE OF MALAYSIA

ARKIB NEGARA MALAYSIA

Projek Pemeliharaan Rekod Elektronik Sektor Awam
(e-SPARK)

Project Documentation

Guidelines on Electronic Records Management

Guidelines on Electronic Records Management

Preface

This Guideline was produced as a result of the e-Spark initiative. Sponsored by the Arkib Negara Malaysia and involving departments and agencies from across the Government of Malaysia, the purpose of this initiative was to develop policies, standards and practices, technical specifications and training plans to enable the Government of Malaysia to manage records in electronic form. Also included was a strategic plan reflecting the roles and responsibilities of public offices and various central and lead agencies. The Arkib Negara Malaysia, within its legislative mandate to facilitate the management of records in any physical form and to acquire, preserve and make available those of archival value, is the lead department responsible for facilitating the government-wide management of electronic records. In this capacity and in cooperation with other central agencies and public offices, it is responsible for issuing standards and guidance to public offices on the management of electronic records.

Guidelines on Electronic Records Management was produced by the Arkib Negara Malaysia to help public offices to manage electronic records. More specific guidelines addressing the management of electronic records in specific environments are also available. These are as follows: ***Managing Electronic Records in the Unstructured Environment, Managing Electronic Records in the Structured Environment,*** and ***Managing Electronic Records in the Web Environment.*** All are available from the Arkib Negara Malaysia.

These guidelines should also be used in conjunction with ***Electronic Records and the Akta Arkib Negara 2003*** (available from the Arkib Negara Malaysia). This publication supports the implementation of the Akta Arkib Negara 2003 and the requirement by government departments not to dispose of their records without the approval of the National Archivist and to transfer records assessed as having archival value to the control of the Arkib Negara Malaysia.

For additional information, please contact:

Arkib Negara Malaysia,
Jalan Duta,
50568 Kuala Lumpur
Tel. 603-62010688
Fax. 603-62015679
Web Site: http://arkib.gov.my

Table of Content

Guidelines on Electronic Records Management

1 Introduction

Records in electronic form are valuable assets that can be lost or destroyed unless they are managed as an asset. Records are created, received and maintained in the conduct of business activities. To support the continuing conduct of business, satisfy applicable legal requirements, and provide necessary accountability, public offices must create and maintain authentic, reliable and usable records, and protect the integrity of those records for as long as they are required to exist. To do this, public offices should institute and carry out a comprehensive records management program, which includes[1]:

a) Determining what records should be created, what information needs to be included in the records, and what level of accuracy is required.

b) Deciding in what form and structure records should be created and captured.

c) Determining requirements for retrieving and using records and how long they need to be kept to satisfy those requirements.

d) Deciding how to organize records so as to support requirements for use.

e) Ensuring that records are created and maintained in accordance with these requirements.

f) Preserving the records and making them accessible over time, in order to meet business and societal requirements.

g) Complying with legal and regulatory requirements, applicable standards and organizational policy.

h) Ensuring that records are retained for as long as required.

The Government of Malaysia and the Arkib Negara Malaysia (ANM) have reached an established level in the area of records management and archives management for paper / conventional records. ANM has the capability and expertise, coupled with strong principles in records management and archives management as well as efficient methods, tools and procedures to ensure that public records and archives are well maintained and preserved.

As the Government of Malaysia shifts increasingly to electronic service delivery channels, ANM is extending its capacity to support the archival management of electronic records. The *Akta Arkib Negara 2003*, which forms the basis of this guideline, amends the *Akta Arkib Negara 1966* to include records created electronically. Where existing international or other standards exist, they inform the guidelines specified below.

[1] These attributes are derived from ISO 15489, *Information and Documentation – Records Management*, 2001

Following this introduction, Section 2 provides an overview of the concepts and definitions that underpin the guidelines described in subsequent sections. Section 3 provides general guidance on the management of electronic records throughout their life cycle (i.e. creation, preservation, use, disposition). Section 4 presents a checklist of management and governance considerations that should be addressed to ensure that a sustainable program for the management of electronic records is in place. Section 5 addresses specific topics such as the management of encrypted records.

Specific guidance on the management of electronic records in specific business process environments can be found in three companion guides:

Managing Electronic Records in the Structured Environment
Managing Electronic Records in the Unstructured Environment
Managing Electronic Records in the Web Environment

For additional information please contact:

Arkib Negara Malaysia,
Jalan Duta,
50568 Kuala Lumpur
Tel. 603-62010688
Fax. 603-62015679
Web Site: http://arkib.gov.my

2 Concepts and Definitions

2.1 Introduction

This Section describes some of the basic concepts associated with recordkeeping and the management of electronic records. It is a foundation section upon which the standards provided in subsequent Sections can be understood more clearly.

According to the Akta Arkib Negara 2003 and in accordance with the Policy on the Management of Electronic Records,

> *"**records**" means materials in written or other form setting out facts or events or otherwise recording information and includes papers, documents, registers, printed materials, books, maps, plans, drawings, photographs, microfilms, cinematograph films, sounds recordings, electronically produced records regardless of physical form or characteristics and any copy thereof;*
>
> *"**public records**" means records officially received or produced by any public office for the conduct of its affairs or by any public officer or employee of a public office in the course of his official duties and includes the records of any Government enterprise and also includes all records which, on the coming into operation of this Act, are in the custody or under the control of the National Archives of Malaysia established under the Akta Arkib Negara 1966 [Act 511];*

Electronic government records are those records that fulfill these criteria and which are created and maintained in electronic format.

2.2 Purpose of a Record

The purpose of a record is to serve as an authoritative, authentic, and reliable source of information and as the means of documenting decisions.

Adequate records enable public offices to[2]:

- Conduct business in an orderly, efficient and accountable manner.
- Help deliver services in a consistent and equitable manner.
- Support and document policy formation and managerial decision-making.

[2] Derived from ISO 15489, *Information and Documentation – Records Management*, 2001

- Provide consistency, continuity and productivity in management and administration.
- Facilitate the effective performance of activities through an organisation.
- Provide continuity in the event of a disaster.
- Meet legislative and regulatory requirements including archival, audit and oversight activities.
- Provide protection and support in litigation including the management of risks associated with the existence of or lack of evidence of organizational activity.
- Protect the interests of the organization and the rights of employees, clients and present and future stakeholders.
- Support and document current and future research and development activities, developments and achievements, as well as historical research.
- Provide evidence of business, personal, and cultural activity.
- Establish business, personal and cultural identity.
- Function as corporate, personal or collective memory.

Records are an integral part of business processes and must be managed and retained for as long as they are needed to support the functions of the government and to provide evidence of decisions and activities (see Figure 2.1).

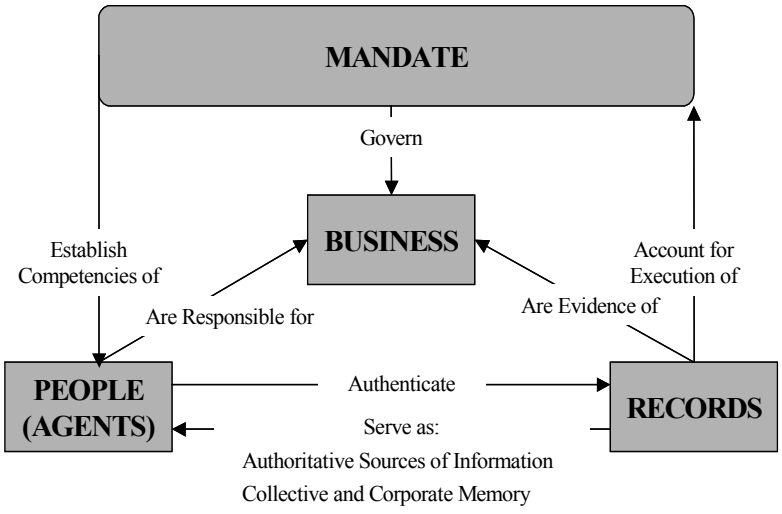


Figure 2.1: Records as an Integral Part of the Business Activity

2.3 Attributes of a Record[3]

In order to serve as reliable evidence of decisions and activities, records must have the following qualities:

2.3.1 Authenticity

An authentic record is one that is proven both to be what it purport to be and to have been created or sent by the person who purports to have created or sent it. To demonstrate the authenticity of records, public offices should implement and document policies and procedures which control the creation, transmission and maintenance of records to ensure that records creators are authorized and identified and that records are protected against unauthorized addition, deletion and alteration. To be authoritative, a record should be created at the time of the transaction or incident to which it relates, or soon afterwards, by individuals who have direct knowledge of the facts or by instruments routinely used within the business to conduct the transaction.

2.3.2 Reliability

A reliable record is one whose contents can be trusted as a full and accurate representation of the transactions, activities or facts to which they attest and can be depended upon in the course of subsequent transactions or activities.

2.3.3 Integrity

The integrity of a record refers to its being complete and unaltered. It is necessary that a record be protected against alteration. Records management policies and procedures should specify what additions or annotations may be made to a record after it is created, under what circumstances additions or annotations may be authorized, and who is authorized to make them. Any authorized annotation or addition to a record made after it is complete should be explicitly indicated as annotations or additions.

2.3.4 Usability

A useable record is one, which can be located, retrieved, presented and interpreted. It should be capable of subsequent presentation as directly connected to the business activity or transaction, which produced it. The contextual linkages of records should carry the information needed for an understanding of the transactions that created and used them. It should be possible to identify a record within the context of broader business activities and

[3] These attributes are derived from ISO 15489, *Information and Documentation – Records Management*, 2001

functions. The links between records that document a sequence of activities should be maintained.

2.3.5 Accuracy, Adequacy and Completeness

A record should correctly reflect what was communicated, decided or done. It should be able to support the needs of the business to which it relates or it evidences so that it can be used for accountability purposes. A record should contain not only the content, but also the metadata necessary to document a transaction, as follows:

- The structure of a record, that is, its physical and logical format and the relationships between the data elements comprising the record, should remain physically or logically intact

- The context in which the record was created, received and used within business should be apparent in the record (including the business process of which the transaction is part, and the participants in the transaction)

- The links between documents, held separately but combining to make up a record, should be present.

2.4 Principles for Electronic Records Management

The following principles govern the management of electronic records:

- Electronic records are assets that need to be managed with the same diligence as any other asset.

- The management of electronic records is not a problem that needs to be solved. Its effective implementation in support of program/ service delivery, decision-making, etc., should be viewed from the perspective of the extent to which it can lead to cost savings, cost avoidance, risk reduction and opportunity gain.

- An electronic records management infrastructure is function driven. The requirements of a government program or strategic direction drive the decisions about what records need to be created, collected, acquired, etc. and how electronic records should be used, preserved and systematically disposed.

- While the introduction of computer technologies will change the nature of the records and may even conceivably lead to the de facto record of Government functions becoming electronic, the management principles remain the same.

- The nature of the work of electronic records management and its associated competencies define the electronic records management community. While registry personnel are central to the community, other communities such as information technology, audit, the officials responsible for the delivery of government programs and services and those involved in the private sector in providing records management technologies and services are also involved and must be considered when developing awareness and education/ training programs.

- The management of electronic records is the responsibility of all individuals.

Electronic records are susceptible to loss and destruction because of:

- The fragility of the media upon which they are recorded.
- The dependency on technology that changes through time.
- The absence of contextual information (metadata) that permits the records to be understood.
- The absence of assigned accountability for the proper management of the records.

If these issues are not addressed then the following negative impacts will result[4]:

- *Reduced program effectiveness and efficiency* when program-related information in electronic records is inaccurate, incomplete or out-of-date.
- *Increased administrative costs* when electronic records collection and storage are duplicated, when they are kept too long or when they cannot be found and must be reconstructed.
- *The inability to assess program impacts* when performance-related electronic records are not kept.
- *Increased legal, financial or political risk* when the evidence contained in electronic records is unavailable or is not credible.
- *Wasted investment in technology* when government is unable to establish trustworthy electronic recordkeeping environments.
- *Gaps in the government's 'corporate memory'* when electronic records with long-term value have not been preserved or are not usable.

[4] These impacts were expressed in, *Case for Action for Information Management*, National Archives of Canada, 2002

2.5 Conditions for Electronic Records Management[5]

The requirements for record keeping that are described in the following section represent a set of conditions that must be met if electronic records are to be authentic and reliable and to serve the purposes for which they were created and retained. They are in the form of a checklist that can be used by program managers and staff, applications systems developers, registry staff, LAN administrators, web masters and others to assess the extent to which these conditions are being met for the capture, maintenance, and preservation of electronic records.

2.5.1 Records are captured

Records have been created by all business transactions.

- Communications in the conduct of business between two people, between a person and a store of information available to others, and between a source of information and a person, generate a record.
- Data interchanged within and between computers under the control of software employed in the conduct of business created a record

Records are identifiable. They are related to a transaction which used all the data in the record and only that data.

- There exists a discrete record, representing the sum of all communications associated with a business transaction.
- All data in the record belongs to the same transaction.
- Each record is uniquely identified.

Records are complete. They contain the content, structure and context generated by the transaction they document.

Records are accurate. The content of records is quality controlled at input to ensure that information in the system correctly reflects what was communicated in the transaction.

Records are understandable. The relationship between elements of information content is represented in a way that supports their intended meaning.

Records are meaningful. The contextual linkages of records are in place to carry information necessary to correctly understand the transactions that created and used them.

[5] The following conditions were adapted from the “Pittsburgh requirements” developed as a result of the project, *Business Acceptable Communications* (also known as the Pittsburgh Project), University of Pittsburgh, 1989-1993.

- The business rules for transactions, which minimally locate the transaction within a business function, are maintained.
- A representation of the source and time of the transaction which generated a record is maintained.
- Links between records which comprised a business activity are retained.

Records are authentic. Authorized records creators originated all records.

- All records have creators which are documented.
- Records creators have been authorized to engage in the business transaction that generated the records.

2.5.2 Records are maintained

Records are preserved. The records continue to reflect content, structure and context within any systems by which the record are retained over time.

Records are inviolate. Records are protected from accidental or intended damage or destruction and from any modification.

- Data within a record are not deleted, altered or lost once the transaction which generated it has occurred.

Records are coherent. The information content and structure of records is retained in re-constructible relations.

- If records are migrated to new software environments, content, structure and context information are linked to software functionality that preserves their executable connections or representations of their relations thus enabling humans to reconstruct the relations that pertained in the original software environment.
- Logical record boundaries are preserved regardless of physical representations.

Records are auditable. The context of the records represents all processes in which the records participated.

- All uses of records are transactions.
- Transactions which index, classify, schedule, file, view, copy, distribute, or move a record without altering it are documented by audit trails attached to the original record.
- Transactions which execute a records disposition instruction whether for retention or destruction are documented by audit trails attached to the original record.

Records are removable. The record's content and the structure supporting the meaning of the content may be deleted by authorized individuals (i.e. in accordance with approved retention and disposal schedules).

- Authority for deletion of record content and structure exists.
- Deletion transactions are documented as audit trails.
- Deletion transactions remove the content and structural information of records without removing audit trails reflecting context.

2.5.3 Records are usable

Records are exportable. Records may be transmitted to other systems without loss of information.

- The export import facility has facilities to determine the elements of records metadata, the record content, the associated history data, etc and the sequence that is exported and then imported.
- Exporting protocols are reversible or the lost functionality is represented in a fashion that produces the same result in the target system as in the originating environment.

Records are accessible. It is possible to output record content, structure and context.

Records are available. It is possible to retrieve records.

Records are renderable. Records are displayed, printed or abstractly represented as they originally appeared at the time of creation and initial receipt.

- The structure of data in a record appears to subsequent users as it appeared to the recipient of the record in the original transaction or a human meaningful representation of that original rendering accompanies the presentation of the original content.

Records are evidential.

- Records reflect the context of their creation and use.
- Human meaningful representation of the contextual audit trail of a record accompanies all displays or printed output.

Records are redactable? Records are masked when it is necessary to deliver censored copies and the version as released is documented in a linked transaction.

- The release of redacted versions of a record is a discrete business transaction.
- The fact of the release of a redacted version of a record is an auditable use of the original record and therefore results in creation of an audit trail with a link to the transaction which released the redaction.

These conditions must be met if the records required in support of the business and accountability requirements of a public office are to be captured, used, and maintained as authentic and reliable records through time.

2.6 Business process environments

These conditions and the means by which they can be addressed need to be situated within the context of the business process environments supported in most public offices. While it is recognized that all three environments are expected to converge over time, most public offices are still supporting environments that are relatively distinct. The environments are as follows:

'Unstructured' Environment where business processes and workflow are not clearly defined, the user has relative autonomy over what information is created, sent and stored (e.g. as e-mail and attachments) and accountability for the management of information (including information in 'records') is unclear. This is the world of e-mail and other electronic documents that are generated without the benefit of structured work processes or rules of the road. Typically it is a user driven world where the user has autonomy concerning what gets created, how it is transmitted and how it is stored and otherwise managed. The absence of workflow within which records/documents (regardless of their physical form) can be placed in a context presents a substantial challenge from a recordkeeping perspective. Electronic recordkeeping solutions tend to be derived from the world of paper based records management.

'Structured' Environment where business processes are typically highly structured, well-established tools and techniques are employed to develop application systems supporting the processes, and accountability for the design, development and maintenance of systems (including the integrity of the data generated in the systems) has been assigned. This is the 'systems' world where the processes for carrying out the business of the public office have been heavily structured, where accountability for the design, development and maintenance of the systems supporting these processes has been assigned and where the accuracy and reliability of the 'data' generated and managed in these systems must be ensured in order to support the overall integrity of the systems. The management of electronic records should work best in this kind of environment because a platform of accountability, defined work processes and business rules and a codified approach to systems and data design has been established. It doesn't always succeed (which is why there are issues - often related to retention, disposition and long-term preservation - connected with this environment) but at least a framework of policies, standards and practices, systems and technologies and people exists to manage the processes and the multiple forms of information (including records) generated by the processes. Usually, in the absence of an adequate understanding of the record keeping issues in this environment, solutions tend to be derived from the world of systems development and data management.

'Web' Environment where work processes are generally associated with the 'publication' and 'communication' of information (though this is changing rapidly with the advent of E-Government initiatives) and the role of the web master is dominant. This is a rapidly evolving environment. It is the world of 'web content' in which, in the earliest stages of web site evolution, organizations find themselves 'publishing' content onto the web (ergo the issues in this environment tend to be derived from the world of communications, publishing, marketing and library services). But in this era of E-Government, they are also finding themselves managing records that have emerged from defined work processes such as those connected with the development of policy (e.g. the preparation of various drafts of a consultation document placed on the web site or the handling of enquiries placed via the e-mail facility featured on most web sites – similar to 'correspondence management'). Pursuant to the agenda established for many e-government initiatives, many organizations are evolving even further by turning their web sites into gateways or portals in order to support on-line transaction processing (e.g. e-filing of tax returns). In the early stages of web site evolution, any record keeping-related issues are expressed as content management issues (e.g. authenticity, reliability, integrity, security, etc.) and solutions tend to be derived from the publishing/communications world. In later stages both the issues and the solutions may be more closely aligned with the worlds of records management, data management and applications systems development. Over the longer term, the 'web' environment will reflect the convergence of multiple business processes, multiple disciplines and multiple (increasingly integrated) solutions.

3 Managing Electronic Records[6]

3.1 Creating Electronic Records

To support work processes, electronic records should be captured into a corporate system that has recordkeeping capability. Capture is the process of placing a document into a recordkeeping system and assigning metadata to describe the record and place it in context, so that the record can be managed over time.

Examples of records are as follows:
- Correspondence relating to formulation and execution of policies and operating procedures.
- Commitments, decisions, or approvals for a course of action.
- Documents that initiate, deliberate, authorize or complete business transactions.
- Work schedule and assignments.
- Agenda and minutes of meetings.
- Drafts of major policies or decisions circulated for comments or approval.
- Final reports or recommendations.
- Documents of legal or financial implications.
- Acknowledgements of receipt of e-mail records that document essential transactions.

Many types of information generated in the office may not be 'records'. Typical examples are as follows:
- Copies or extracts of documents that are published or downloaded and distributed for information or reference purposes.
- Phone message slips
- Electronic copy of a record of which the paper copy has been filed

Trends such as decentralization, the increasing use of technology in administrative processes, and inadequate control over outsourcing arrangements have created challenges for the systematic creation and keeping of records. Conscious effort is required to ensure that records supporting business activities are created and captured in recordkeeping systems. The procedures and practices a public office establishes to capture its electronic records will depend on the recordkeeping systems in use, the types of electronic records generated and the specific recordkeeping requirements the public office must satisfy.

Each public office produces numerous types of electronic records during the course of its business activities. Any procedures developed to capture those records into recordkeeping systems will need to cover all common digital objects (e.g. word-processed documents and spreadsheets) while retaining a degree of flexibility to cater for non-standard data formats (e.g. vector graphics).

[6] Much of the guidance that follows was derived from *Digital Recordkeeping: Guidelines for Creating, Managing, and Preserving Digital Rec*ords, National Archives of Australia, consultation draft, May, 2004

The skills and experience of various staff, including information and records management professionals, information technology specialists and others may be needed. Public offices with electronic document and records management software should be able to store most electronic records in their native format within the system.

Capture of electronic records within a paper-based or hybrid recordkeeping system presents more difficulty and should be carefully considered by public offices. Two options, neither of which is ideal, are:

- Assigning an appropriate record number to electronic records within the system and then storing them separately.
- Printing records such as email and word-processed documents and attaching them to the relevant hardcopy file.

Approaches such as these may provide a cost-effective interim procedure while a more comprehensive solution is being developed.

3.1.1 Creating Information About Electronic Records

Classification of business activities acts as a powerful tool to assist the conduct of business and in many of the processes involved in the management of records by:

- Providing linkages between individual records which accumulate to provide a continuous record of activity.
- Ensuring records are named in a consistent manner over time.
- Assisting in the retrieval of all records relating to a particular function or activity.
- Determining security protection and access appropriate for sets of records.
- Allocating user permissions for access to or action on particular groups of records.
- Distributing responsibility for management of particular sets of records.
- Distributing records for action.
- Determining appropriate retention periods and disposition actions for records.

Metadata is data describing the context, content and structure of records and their management over time. Metadata allows users to control, manage, find, understand and preserve records over time. Some examples of metadata are:

- The title of a record
- The subject it covers
- Its format
- The date the record is created
- The history of its use
- Details of its disposal.

There are two main categories of metadata that are used to manage electronic records: recordkeeping metadata and resource discovery metadata.

Recordkeeping metadata is structured or semi-structured information that enables the creation, registration, classification, access, preservation and disposal of records through time and across domains. Recordkeeping metadata can identify, authenticate, and contextualize records and the people, processes and systems that create, manage, maintain and use them.

For electronic records to be preserved over time, adequate recordkeeping metadata must be created, captured and maintained. Some metadata may need to be kept for long-term accountability or transfer to the Arkib Negara Malaysia. Other metadata may be destroyed at the time of the records' disposal.

One of the primary uses of metadata is to assist in the description of resources and improve methods of information retrieval. **Metadata for resource discovery** overlaps with and extends beyond the descriptive elements of recordkeeping metadata. Resource Discovery metadata can improve the accessibility of websites, intranets, and web-based services.

The different types of metadata are not mutually exclusive. Particular metadata schemas can serve more than one purpose and there is often overlap and interrelationships between metadata schemas. For example, many of the elements required for resource discovery are also used for recordkeeping purposes. Conversely, recordkeeping metadata can be the basis for a classification scheme, controlled vocabulary or thesaurus. These tools help staff choose terms for indexing, titling and retrieving records.

Capturing and maintaining good recordkeeping metadata supports digital recordkeeping by:

- Protecting records as evidence and ensuring their accessibility and usability.
- Ensuring the authenticity, reliability and integrity of electronic records.
- Enabling the efficient retrieval of electronic records.
- Providing logical links between electronic records and the context of their creation, and maintaining the links in a structured, reliable and meaningful way.
- Allowing timely destruction of temporary-value records when business use has ceased.
- Providing information about technical dependencies, to help ensure digital records' long-term preservation and usability.

Recordkeeping metadata will generally be identified, and/or created when digital records are captured into recordkeeping systems. This defines the point at which the information formally becomes a record, fixes it in its context and enables its appropriate management over time. Metadata collected at the point of capture of a digital record should document its content, structure and the context in which it was created.

Some metadata may be applied at a system level. For example, all records within a finance system will share the same metadata about the organization creating the record, and the business activity being documented. This metadata can be automatically applied to all

records generated within the finance system. Other metadata will be generated as time progresses. Metadata related to business and recordkeeping processes will be added to a digital record during its lifetime. Examples include History of Use (when the record was last viewed, whether it was accessed illegally), Location and Disposal status. Such metadata ensures the continued authenticity, security and integrity of the record.

Recordkeeping and business information systems should be designed and implemented with the necessary infrastructure to generate and capture appropriate metadata. Capture and maintenance of metadata should occur as a normal part of business and recordkeeping operations. Where possible, the capture of metadata should be automated. Ideally, systems design should enable the greatest scope for automating the creation and capture of metadata. The greater the automation, the less likely it will be an intrusion on the daily activities of staff. Automation also ensures consistent interpretation of metadata schemas and the capture of more standard metadata, which facilitates records retrieval.

In many systems, it is likely that some metadata will be entered manually. Staff will require appropriate training and support to feel confident choosing titles or indexing terms as necessary. Simple procedures and systems that assist users to create metadata will lead to more consistency. Some applications provide semi-automated metadata capture. For example, when capturing an email, certain fields may be populated from the header. Users can be prompted to accept or override the data before a record is formally captured into the system.

Metadata required to support electronic records may be captured and managed in several ways. The metadata can be:

- Captured and managed within the recordkeeping or business information system in which the digital record is created and stored.
- Captured into, and managed within, a separate metadata management system and linked to the relevant digital record.
- Encapsulated with the digital record, and managed as an integral part of it.

Systems that embed or encapsulate metadata into electronic records have several advantages. They enable electronic records to become ‘self-describing’ and remove the need for retention of metadata in parallel systems. However, this approach has disadvantages for the preservation of long-term records. There may be difficulties separating the data object from its metadata at a later date. Problems may arise when trying to maintain the metadata for disposed records, or converting a digital record to an archival format.

Public offices should develop policies and practices to ensure that metadata is created and maintained in an appropriate manner. The aim is to standardize the metadata. Policies and procedures should be articulated in the overall recordkeeping and information management strategy for the organization.

Policies and practices on managing metadata should:

- Assign roles and responsibilities for capturing and managing metadata.
- Identify metadata elements to be captured.
- Establish when and how metadata is to be captured.
- Determine how long metadata needs to be retained.
- Detail how metadata is to be stored, including consideration of any persistent linkages between metadata elements and the records to which they relate.
- Ensure that storage is secure and an audit trail of access, usage, and alterations or additions are kept to monitor the integrity and authenticity of the metadata.
- Include adequate backup procedures and recovery mechanisms and a consideration of disaster management.
- Provide for the preservation of metadata for as long as it is required.

3.2 Determining How Long to Keep Electronic Records

The retention period of a record should:

- Meet current and future business needs by:
    - Retaining information concerning past and present decisions and activities as part of the corporate memory to inform present and future decisions and activities.
    - Retaining evidence of past and present activities to meet accountability obligations.
    - Eliminating, as early as possible and in an orderly way, records which are no longer required.
    - Retaining the context of the record which will allow future users to interpret the validity of the records that earlier systems captured and managed.
- Comply with legal requirements, by ensuring that the regulatory environment applicable to records management for specific business activities is documented, understood and implemented.
- Meet the current and future needs of external stakeholders by :
    - Identifying the enforceable or legitimate interests that stakeholders may have in preserving the records for longer than they are required by the public office itself. They may include stakeholders such as business partners, clients and other people affected by the organization's decisions or actions, and others to whom the organization should make its records available to meet accountability requirements, such as auditors, regulatory authorities and investigative bodies, archives authorities or researchers.

- Identifying and assessing legal, financial, political, social or other positive gains from preserving records to serve the interests of research and society as a whole.
- Following regulations of the competent archival authority where applicable.

Records identified for continuing retention are likely to be those which :

- Provide evidence and information about the public office's policies and actions.
- Provide evidence and information about the public office's interaction with the client community it served.
- Document the rights and obligations of individuals.
- Contribute to the building of a public office's memory for scientific, cultural or historical purposes.
- Contain evidence and information about activities of interest to internal and external stakeholders.

An electronic record must be managed, and remain accessible, for its lifetime. How long an electronic record needs to be kept will influence its management. Given the vulnerable nature of most digital media and the frequency of technology change, 'long term' for electronic records generally means longer than one generation of technology. Electronic records that must be retained for the long term will require active management to ensure their continued accessibility.

3.3 Storing Electronic Records

To ensure the ongoing protection of electronic records, public offices require efficient and effective means for maintaining, handling, and storing electronic records – both active and inactive – over time. Policies, guidelines and procedures for the storage of electronic records should be an integral component of a public office's recordkeeping framework.

There are three ways in which public offices may store electronic records – online, offline or near-line.

- **Online** – Online records can be contained on a range of storage devices (e.g. mainframe storage, network attached storage or PC hard drive) that are available for immediate retrieval and access. Generally, records stored online will be active electronic records – i.e. records that are regularly required for business purposes. Electronic messaging systems and word-processed documents saved to the network server fall into this category.
- **Offline** – Offline electronic records are contained on a system or storage device that is not directly accessible through the public office's network and which requires human

intervention in order to be made accessible to users. Electronic records that are stored offline are usually retained on removable digital storage media (e.g. magnetic tape, CD, DVD) and are generally inactive electronic records not regularly required for business purposes. Offline electronic records may be stored offsite as part of an agency's business continuity plan. Electronic records stored offline are not immediately available for use. Public offices must take responsibility for monitoring and guarding against environmental degradation and changes in technology that may adversely affect the storage media employed.

- **Near-line** – Near-line storage of electronic records means the records are contained on removable digital storage media, but remain relatively accessible through automated systems connected to the network. These electronic records are technically considered to be offline. The use of systems such as CD jukebox or magnetic tape silos allow them to be made available through public office networks, in relatively short periods of time and without the need for human intervention (i.e. staff are not required to physically retrieve the storage media on which the required information is retained).

Generally, electronic records will begin life as online records and, as the immediate business need to refer to them diminishes over time, they will be moved to either near-line or offline storage, depending upon the technology available to the public office, the ongoing relevance and value of the records and their retention requirements.

Based on relevant recordkeeping and business requirements, public offices must decide which electronic records are to be captured and maintained online and which electronic records can be retained in near-line or offline storage.

Electronic records of vital significance to a public office, as well as electronic records required for long-term retention within public offices, and electronic records of archival value, should be stored online. Online storage devices, such as network storage devices and mainframe storage, have the following advantages:

- Electronic records stored online will, in most cases, be retained on the magnetic hard drives that form a public office's network, where they will be readily accessible to users and can be maintained and controlled as an integral part of the public office's recordkeeping system.
- Large storage capacities allow for significant quantities of electronic records to be retained on a single storage device.
- Regular integrity checks of electronic records can be more readily performed and, in some instances, it may be possible to automate these tasks.
- Electronic records stored online have a greater likelihood of being identified and included within any changes made to the IT systems of public offices, such as system-wide migration processes.
- Online storage devices need not be linked directly to a public office's network. Where security concerns, business considerations or other factors warrant, public offices may opt to establish standalone online storage systems.
- Increasingly, online storage systems can support sophisticated automated techniques and redundant designs that aid electronic records control, monitoring and backup.

The automated nature of near-line systems means that they share many of the advantages of online systems, even though the electronic records stored on near-line systems are retained on physical storage media such as DVDs, CDs and magnetic tapes. Where it is not possible for electronic records to be maintained online, agencies are encouraged to use near-line storage devices, such as CD jukeboxes and magnetic tape silos.

For storing electronic records, the Arkib Negara Malaysia does not recommend CDs, DVDs, magnetic tape and other removable digital media formats that are physically maintained, but not accessible from active computer systems. Offline digital storage devices are suitable only for storing relatively low-value electronic records and are not recommended for long-term electronic records, vital records or records identified as being of archival value.

Offline digital storage devices present the following challenges.

- The records are not immediately accessible to users, as the storage media must first be physically retrieved.
- Individual media need to be labeled and stored in a manner that permits them to be easily accessed. Failure to adequately store removable digital media formats may result in electronic records being physically misplaced or lost.
- Removable media are less likely to be routinely accessed and may be missed when conducting routine integrity checks.
- Similarly, offline media are often overlooked when public office systems are upgraded and electronic records are migrated to new formats. This can result in the electronic records contained on offline media becoming inaccessible.
- Device failure is only detected when an attempt is made to use the records.

Regardless of whether public offices adopt an online, offline or near-line storage method, they should take the following into account before selecting a specific storage device.

- How often and how quickly will the records need to be accessed?
- Is the proposed storage device versatile and has it the capacity to accommodate the size, number and complexity of electronic records to be stored?
- Is the longevity, reliability and durability of the proposed storage device sufficient to meet the required retention periods for the electronic records it is to contain? In the case of long-term electronic records, the selected format should be robust and have a clearly definable migration path and widespread industry support to improve the chances of forward compatibility.
- Are the technical standards associated with the storage device technology open source? Proprietary storage formats may be less widespread and less likely to be sustained and supported over time.
- Will the selected storage device have any special physical or environmental storage requirements?
- Do the assessed costs and benefits of the proposed storage device suit the needs of the public office and the electronic records to be stored? Costs include migrating records, the storage device and associated hardware, and any training that may be required.

To keep electronic records over time, public offices should consider not only the storage devices, but also the facilities for housing them and the computer systems that generate the records.

Electronic records are more vulnerable than paper records, so public offices need to devote more time and resources to their accommodation. The earlier a public office can plan for the storage and retention of electronic records, the better, in terms of the records' longevity. Storage conditions should support record protection, make records accessible, and be cost effective. Digital storage devices are susceptible to fluctuations in humidity, temperature and radiation, so the Arkib Negara Malaysia strongly advises that stable environmental conditions be maintained.

Periodically, public offices should undertake risk analysis to ensure that storage conditions are appropriate for both digital storage devices and information systems. Public offices should also perform regular and ongoing integrity checks of all digital storage devices, such as data object checksums, to ensure that no deterioration or data loss is occurring.

Digital storage technology is always improving, with new digital storage devices evolving to replace older, outmoded devices. Public offices should be aware of developments in storage technologies with a view to ensuring that there are clear migration paths for the storage device technology they currently employ.

The life expectancy of offline digital media varies depending on the format and quality of the media, storage conditions, and handling and treatment. Damage resulting from deterioration will differ depending on the types of media involved and may vary from corrupt sectors on a disk, resulting in one or more files becoming inaccessible, to the complete loss of all information on the media.

Given the potential for electronic records to be lost as a result of media deterioration, it is critical that public offices monitor digital media integrity and schedule periodic refreshing of media. Specific advice on the care, handling and maintenance of digital storage media is available in Appendix 3.

Online, offline and near-line digital storage devices have limited life expectancy. It is imperative to monitor them continuously and refresh them periodically – i.e. migrate the data to a suitable replacement. Examples of migration include the transfer of digital records from an outmoded online storage system to a replacement online system, or the transfer of records stored on an outmoded offline digital media format, such as a floppy disk, to a replacement media format, such as a compact disk. The greatest problem in planning for the refreshment of digital storage devices, is identifying when it is appropriate to replace them. Unlike paper-based records, deterioration of digital storage devices does not become obvious until the point of data loss and, by that stage, it can often be too late to salvage the records.

The fact that most digital storage devices have only emerged recently, means that the life expectancy for these devices is largely unproven. Rapid cycles of technological obsolescence occurring within the IT industry present the possibility that digital storage devices may well become outmoded, unsupported and obsolete due to unavailability of the software and hardware required to access the records stored on them long before the storage devices themselves physically degrade.

Public offices are therefore advised to be conservative when planning for the refreshment of storage devices, and to err on the side of caution, rather than risk the loss of electronic records from storage device deterioration. In deciding when to refresh storage devices, public office staff will need to consider the following factors:

- Vendor claims of storage device life expectancy (preferably supported by evidence from independent tests).
- Technological advancements that make the current storage device obsolete.
- Ready access to equipment capable of reading and rendering the electronic record contained on the current storage device.
- Relevant standards (e.g. ISO 18921 on estimating the life expectancy of compact disks based on the effects of temperature and relative humidity).
- The results of ongoing internal storage device integrity checks.

When contemplating refreshing digital storage devices, public offices should consider the selection criteria for digital storage devices. Where electronic records are transferred to a new digital storage device, the content, context and format of the electronic records contained on the existing storage device must not be altered as a result of the transfer.

Standard error checking techniques should be used to assess the quality of the blank storage device to be used. And after the transfer has been completed (and before the source records are destroyed), spot checks should be undertaken to ensure that the electronic records have been reliably and accurately transferred to the new device. Verification techniques, such as checksums, should be used to confirm digital record integrity.

After each transfer it is advisable to perform a test restoration of the data to verify the success of the process and ensure that the electronic records are still accessible.

Where digital storage devices are not refreshed in a timely manner there is a significant chance that the electronic records they contain will become corrupted and inaccessible. Allowing electronic records to become inaccessible may be viewed as a breach of the *Akta Arkib Negara 2003*.

In cases where electronic records cannot be accessed due to the failure or corruption of the storage device, public offices should seek assistance from commercial data recovery services and take all reasonable steps to recover the electronic records. The feasibility and cost of recovering the lost electronic records will depend on the type of digital storage device used, the level of degradation and the complexity of the recovery process required.

While it may not always be possible to completely recover electronic records from damaged storage devices, in most cases there will be a reasonable prospect of at least partial success. Public offices will need to balance the value and significance of the lost or damaged digital records with the cost of their recovery. Where the electronic records involved are of temporary value, and the loss of the records does not pose an unacceptable risk to the agency, the cost of recovery may not be justified.

In cases where electronic records of archival value are concerned every effort should be made to recover the records. Public offices faced with the task of recovering inaccessible electronic records of archival value should contact the Arkib Negara Malaysia for further assistance.

3.4 Securing Electronic Records

Security is important for all records. The manipulable nature of electronic records means that, in the absence of appropriate safeguards, it is relatively easy to alter or delete them – whether intentionally or unintentionally. Alterations to electronic records can be virtually undetectable, undermining their evidential value as records.

When implementing systems, public offices must therefore take special care to ensure they are secure, reliable and capable of producing records that are acceptable for legal, audit and other purposes. The remainder of this sub-section describes security measures to be taken to prevent data loss, data corruption, unauthorized data access and to ensure the integrity, reliability
and confidentiality of electronic records.

Security regulations require public offices to consider the security needs of their systems and to devise policies and plans to ensure that systems are appropriately protected. Public offices are required to prepare a security plan that describes the security mechanisms and procedures that have been implemented to protect electronic records and systems.

As a first step towards developing a public office security plan, formal threat and risk assessments should be conducted on all computer systems (including information systems, recordkeeping systems and online services provided by the agency) by an appropriately qualified body or agency. System vulnerabilities and potential threats should be identified and strategies developed and implemented to reduce the likelihood of security breaches occurring.

The following are some basic practices and protocols public offices may adopt to ensure they maintain adequate security for their electronic records and systems. This list is not exhaustive. Public offices should select a combination of methods to suit their needs.

- Limit access to electronic records, and the systems on which those records are created and kept, to authorized personnel in order to protect the integrity of the records and prevent unlawful alteration or destruction of records.
- Establish network security systems, such as firewalls, to protect against unauthorized access (e.g. hackers) to systems that are accessible through external connections, such as the Internet.
- Install appropriate gateway filter software on messaging systems, and ensure that filter definitions are regularly updated, to protect against spam, denial of service attacks and malicious code, such as computer viruses.
- Implement public key infrastructure (PKI) encryption technologies to ensure secure transmission of electronic records to external parties.
- 'Lock' final electronic records to prevent any subsequent alterations or inadvertent destruction (e.g. finalizing records as 'read-only' within an electronic recordkeeping system).
- Use digital signature technologies to authenticate electronic records and provide security and confidence in authorship.
- Store vital electronic records either offline or on systems without external links.
- Establish appropriate systems backup procedures and disaster recovery strategies to protect against loss of electronic records.
- Develop and implement audit trails to detect who accesses a system, whether prescribed security procedures were followed and whether fraud or unauthorized acts have occurred, or might occur.

The level of physical storage security standards for computer rooms, workstations and digital media storage areas will differ depending on the value and sensitivity of the information held by the agency and the risk posed by the potential loss of the records. Approved security standards and practices should be used to provide benchmarks and guidance on electronic records security within public offices. Security practices should be periodically reviewed and system log files interrogated to identify any potential attempts to breach systems security – as well as any previously undetected breaches. The relevant public office manager should develop incident reporting systems and be familiar with the appropriate standards and procedures so that breaches of security can be reported in a timely manner and appropriate action taken to prevent further breaches.

Electronic records provide evidence of business activity. For electronic records to retain their evidential value, and be admissible as evidence in court, systems and practices must prevent the unauthorized alteration of electronic records, and so ensure their continued authenticity.

To guarantee the authenticity of electronic records, systems and procedures should be capable of establishing:

- If electronic records have been altered.
- The reliability of software applications creating electronic records.
- The time and date of creation and alteration of electronic records.
- The identity of the author of a digital record.

- The safe custody and handling of records.

Version control is a useful tool for preserving the authenticity of electronic records. Electronic source records should be clearly distinguished from any subsequent copies. Identification may be achieved through labeling of records or by time and date stamps.

To provide evidence of business activities or action taken, agencies must be able to clearly demonstrate the provenance of electronic records. This includes establishing the original conditions for the creation of the record, such as date and time of creation, software application integrity and the author or sender of a record. The ability to track when the record was last altered, by whom, and the 'chain of custody' (who was responsible for the record) will also support a record's evidential value.

Clearly implemented policies and procedures demonstrate that a public office has protected the provenance of its electronic records. In some instances, authenticity may be demonstrated if access to electronic records is restricted to authorized persons or applications. In such cases, there must be security mechanisms to prevent unauthorized persons or applications accessing the electronic record. Audit trails should be able to verify that electronic records have not been accessed inappropriately or illegally.

Alternatively, public offices may make use of standards-based cryptographic techniques to authenticate authorship, enable secure transmission and provide strong evidence that a particular electronic record has not been altered, or that a copy of the record is identical to the original.

Electronic records should be decrypted before being captured into secure recordkeeping systems.

Public offices should take additional care to ensure that their security and authentication mechanisms do not inadvertently make electronic records inaccessible in the long term and that the evidential value of the records does not diminish over time. This is particularly important for records of archival value.

Public offices should address the following considerations when applying security and authentication practices and protocols to electronic records.

- If manipulation of data is required (e.g. encrypting a file to send via email), the process should be applied to a copy of the source record. The source record should be maintained separately in a secure recordkeeping system. This will safeguard records of long-term or archival value in the event that data loss occurs during manipulation or the file becomes inaccessible.
- Access controls should be applied and maintained within a recordkeeping system. Staff should be discouraged from using software functions to create passwords or limit access to business records. This includes specifying who can read or alter a document, preventing copying or printing, or setting an expiration date. Documents that have been password-protected or otherwise restricted should not be captured into a recordkeeping

system while the restrictions are still in place. There is a considerable risk that records will become inaccessible as staff changes occur and passwords are forgotten over time. Unrestricted records should be captured into recordkeeping systems. Authorized users can then apply access controls, in accordance with business rules.

- Metadata attesting to the validity of a digital signature, where a digital record has been authenticated using such technology, should be captured and maintained for as long as required. If such information is not kept, the evidential value of the record may be undermined.
- Electronic records that have been encrypted should be decrypted prior to capture in a secure recordkeeping system. Metadata relating to the encryption and authentication process should be captured and maintained for as long as required. If encrypted records are captured and kept there is a considerable risk they will become inaccessible.

3.5 Preserving Electronic Records for the Long Term

Considering the problems of technological change, and the potential instability of digital storage media, 'long term' may not be very long. When applied to the preservation of electronic records, 'long term' usually means 'greater than one generation of technology'.

Many records have retention periods greater than one generation of technology. It is important that these records are preserved and accessible for use in daily business. Long-term records support strategic planning and decision-making. They act as corporate memory, reducing duplication of work and improving business efficiency. There may also be evidentiary reasons to keep electronic records for extended periods, as part of a risk minimization strategy. Inaccessible records may expose agencies to accountability failures and potentially costly consequences, such as legal action.

All public offices should develop strategies to preserve/migrate electronic records, and to ensure that all digital records are captured into a corporate recordkeeping system. Long-term maintenance is particularly significant for electronic records of archival value. Inadequate preservation strategies can render electronic records inaccessible and unusable. Allowing electronic records to become inaccessible may be considered a breach of the Akta Arkib Negara 2003.

Accessibility requirements apply to all electronic records, not just those of archival value. Electronic records must remain accessible for as long as they are required.

3.5.1 Planning for technological obsolescence

Electronic records are dependent on various combinations of hardware, software and media to retain their content, context and structure. Public offices must ensure that the technology required to render a digital record usable and accessible is available. It is not sufficient to simply retain records in digital format; the records and associated metadata must be in a format that is viewable with current technology.

Computer technology is subject to ongoing technological obsolescence, with both hardware and software quickly becoming outdated as new upgrades and versions come onto the market. This can result in electronic records created using older hardware and software becoming inaccessible in their original form after a relatively short period of time. Public offices that need to retain electronic records for the long term should plan for technological obsolescence by ensuring that records can be copied, reformatted, converted or migrated across successive generations of computer technology.

Such planning involves considering hardware, software, operating systems and storage devices. Public offices need to consider a number of interrelated software and hardware issues when preserving electronic records, including:

- The proprietary, platform-specific nature of many software applications and the likelihood of their continued availability
- The cost of maintaining access to obsolete formats (including operating system software and licensing fees) for a system no longer in active use
- The estimated physical and/or commercial life of the media on which digital records and related metadata are stored
- The long-term availability of the hardware and operating system platforms needed to access records stored on different types of media.

The need to plan for technological obsolescence and provide for the preservation of electronic records should be incorporated, through a formal electronic records preservation strategy, within the governance frameworks for information systems. The preservation strategy should outline the approach adopted by the agency for the preservation of its electronic records. There are several common techniques.

3.5.2 Creating an electronic records preservation strategy

In order to adequately manage the preservation of electronic records over time, and ensure their continued accessibility, public offices must be proactive. They should develop and implement organization-wide strategies targeted at identifying, managing, preserving, and ensuring continued access to electronic records.

An effective electronic records preservation strategy should incorporate formal policies and procedures governing the agency's approach to the long-term management of its electronic records and establish processes to ensure their ongoing maintenance.

A public office's electronic records preservation strategy must reflect its legislative obligations, industry standards and best practices. An electronic records preservation strategy should be supported by a plan for its implementation that is promulgated to relevant staff. This can be achieved by:

- Formulating policies, procedures and guidelines to provide a formal framework within the organization for the implementation of the strategy.
- Providing manuals, information and reference sheets, and training for staff to ensure the preservation strategy is correctly implemented. Depending on the approach adopted, this may require training for all operational areas, not simply for records and IT staff.
- A plan clearly setting how and by whom the preservation activities identified in the strategy will be audited.

Public offices should assign responsibility for the management of long-term electronic records to an appropriate area within the organization where staff have relevant skills and qualifications. This will generally be a specialized information or knowledge management unit headed by a senior information officer. Responsibility for policy and procedure formulation, implementation of strategies to preserve electronic records, evaluation, monitoring and review of processes, and delivery of training should rest with this area.

Public offices should ensure that their electronic records preservation strategy takes into account electronic records that may be created and managed by outsource providers and that these contractors are also required to actively comply with the agency's long-term electronic records preservation strategy.

3.5.3 Techniques for electronic records preservation

Some early approaches to electronic records preservation relied on storing records in their original format on physical media – much like boxes are used for the storage and protection of paper records. However, magnetic tapes and disks, and optical storage disks (e.g. CDs and DVDs) are manufactured for short-term storage of digital objects, not long-term archival retention. The greatest concern for this method of preservation, in addition to the relatively short life span of digital media, is the obsolescence of the hardware and software used to access the records. Rapid change in the IT industry and the move from science-based development to commercial development of software and hardware systems, have meant that media rapidly become inaccessible.

Consequently, this approach to digital preservation has proven to be wholly inadequate and the Arkib Negara Malaysia strongly advises against this preservation strategy. The most common techniques for electronic records preservation can be grouped into three broad

categories. Any one or a combination of these may form the basis for an agency's electronic records preservation strategy.

Migration

Migration relies on a program of constant transferal (migration) of electronic records from older or obsolete hardware and software configurations or generations, to current configurations or generations in order to maintain accessibility. This strategy avoids the obsolescence issues of the physical media solution, preserving the functionality of the electronic records and enabling users to retain access to the records – but requires a substantial investment in resources to undertake the repetitive migration work involved. Furthermore, some characteristics of the original data format may not be retained through the migration process and, as a result, users will lose access to characteristics of the source record that may be important to its meaning.

Conversion

Conversion is the process of transferring electronic records from their original data format to a standardized, long-term preservation format (also known as an archival data format). Conversion is also referred to as 'normalization', 'stabilization' and 'standardization'.

The conversion process is a form of migration. However, instead of migrating from an outmoded data format to a current data format, the original data format is migrated to an archival data format. Generally, archival data formats are open source, nonproprietary formats that provide greater potential longevity and are less restrictive than proprietary formats. Conversion reduces the need for repeated migrations.

Encapsulation

Encapsulation requires metadata to be bundled with, or embedded into, the digital object. The metadata allows the record to be intellectually understood and technologically accessed in the future. A viewer is then required to display the records. This packaging of contextual information ensures the integrity and authenticity of records over time. However, there is some risk that important metadata may be overlooked during encapsulation.

On its own, encapsulation cannot preserve electronic records. This technique should be used in conjunction with migration or emulation to ensure the ongoing accessibility of the records.

Emulation

Emulation uses software to recreate the digital record's original operating environment to enable the original performance of the software to be recreated on current computer systems. The result is that the original data format is preserved and may be accessed in an environment that allows for the recreation of the original 'look and feel' of the record. The downside to the emulation approach is that the creation of the underlying emulator software

is costly, requiring highly skilled computer programmers to write the necessary code. Furthermore, the intellectual property and copyright issues associated with the emulation of proprietary software may undermine the effectiveness and sustainability of the approach.

3.5.4 Choosing an approach to electronic records preservation

Public offices should consider the following factors when choosing an approach to electronic records preservation:

- Cost of implementation, including cyclical costs for ongoing preservation treatments.
- Technical complexity of the selected approach and the capacity of the public office to support the approach over time (both technically and financially).
- Compatibility with existing hardware and software.
- Impact on business operations (e.g. whether the approach requires changing corporate work practices).
- Overall effectiveness and robustness of the approach in protecting the integrity, accessibility and functionality of the public office's electronic records over time.

3.5.5 When should a digital preservation treatment be applied?

To maximize the long-term preservation prospects for electronic records, preservation techniques must be applied as soon as practical, preferably while the records are still accessible. Most data formats have a limited window of opportunity during which preservation treatments can be applied before the format becomes outmoded and inaccessible. The sooner a public office addresses preservation issues and determines and implements an appropriate preservation approach, the higher the probability that the electronic records will be successfully preserved.

Public offices are therefore encouraged to be proactive in pursuing their electronic records preservation strategies and to determine and implement appropriate electronic records preservation techniques before their electronic records become outmoded and inaccessible.

Preservation treatments are often undertaken reactively in response to the immediate business needs of a public office, rather than as part of a considered solution to long-term electronic records retention requirements. Such processes may be technology-driven exercises, initiated in response to changes in IT infrastructure or as a consequence of adopting new or upgraded software. In such cases, preservation treatments are undertaken primarily to ensure that existing electronic records, particularly active core business records, are transferred from their original format into a new format capable of functioning within the upgraded IT environment.

3.5.6 Planning to implement a preservation strategy

Periodic preservation treatments (such as migration) are often applied to electronic records without necessarily considering the long-term implications for the integrity of the records. If sufficient care is not taken to protect the integrity and authenticity of the records, migrating software and hardware systems can jeopardize their evidential value.

Public offices that apply preservation treatments to data formats without properly assessing the processes, risk the loss or limitation of the functionality, format, structure and content of their electronic records and the potential loss of metadata relating to the records.

Planning for the preservation of electronic records will allow public offices to retain the functionality and integrity of electronic records after successive upgrades of hardware and software. Development of preservation strategies, and the selection of an appropriate approach, should be the result of a collaborative effort between the records and IT sections within an agency. Best practice recordkeeping issues need to be carefully considered, and the input of records and information personnel taken into account, before any preservation processes are applied to electronic records.

3.5.7 Implementing the preservation strategy

Although the three main preservation techniques – migration, encapsulation and emulation – differ substantially in their method of preserving electronic records, they share common ground in the process of implementation. The following steps outline the implementation process.

Identify records requiring preservation – Identify and select electronic records that require the application of preservation treatments in order to ensure their continued accessibility.

Research technical solutions – Investigate the hardware and software technologies required to successfully implement the public office's preferred preservation approach. In the case of emulation, this may involve the development of specialized software capable of re-creating the source records within a new computer environment. In the case of migration, this may involve identifying suitable migration paths (i.e. software applications with sufficient backward compatibility to transfer source records from an outmoded data format to a current data format). In the case of encapsulation, this may involve software with the ability to embed metadata or
'package' it with the record.

Test proposed solution – Before a preservation approach is fully implemented, staff of the public office must conduct comprehensive testing of the technical processes. Testing should be performed on duplicates of source records.

Back up records identified for preservation – Prior to implementation, all electronic records identified for preservation treatment should be backed up. The integrity of the duplicates should be verified before they are removed to a secure storage area. These duplicate source records should not be subjected to a preservation process and will serve as master copies should the selected preservation treatment be unsuccessful.

Apply the preservation treatment – After successful testing, the treatment should be applied to all electronic records identified for preservation treatment. For migration and encapsulation techniques, this would entail applying preservation treatments to the source records, thereby altering their format. For an emulation-based technique, the records identified for preservation would be transferred to the new environment – without altering the records themselves.

Audit the integrity of preserved records – Following implementation of the preservation process, the preserved records should be subjected to rigorous testing to ensure that any reduction in functionality, or loss of content, structure or format, is within previously set limits of acceptability. The integrity of all relevant metadata associated with the preserved records should be verified. Metadata should also be updated to record the preservation treatment.
If the records cannot be verified, the preservation process will need to be repeated on new duplicates of the source records. In some instances, the preservation strategy itself may require re-evaluation.

Destroy source records where appropriate – Once the preservation process has been completed and the integrity of the preserved records has been verified, public offices may destroy the duplicate source records.

Establish monitoring regimes – The integrity of the preserved records, their functionality, structure, content and context, and associated metadata, should be monitored periodically following preservation to ensure the stability of the preserved records and to identify when subsequent preservation treatments are required.

Please note that, if it appears likely at any stage during the application of a preservation treatment that electronic records of archival value may be lost or significantly altered as a result of the preservation process, the Arkib Negara Malaysia should be consulted immediately so that alternative arrangements may be considered.

Public offices experiencing significant difficulty in ensuring the continued accessibility of their electronic records should contact the Arkib Negara Malaysia for advice.

3.5.8 Requirements for a successful preservation strategy

A successful preservation strategy ensures the continued integrity of electronic records, as well as their continued accessibility and functionality. The preservation of integrity requires that the records, and their associated metadata, remain reliable, complete and authentic.

The following steps will ensure successful preservation of electronic records.

- Care is taken in selecting and testing software applications and hardware required for preservation processes.
- Where possible, non-proprietary, fully documented, open source data formats are used – particularly when implementing migration-based preservation techniques. Proprietary data formats are not recommended for long-term storage of records.
- Preservation processes are applied systematically to all electronic records, both current and non-current, retained by an agency. Failure to include non-current electronic records can result in their inaccessibility.
- All relevant metadata (for the records and the preservation process) is captured at the time of preservation.
- Preservation processes are fully documented and the documentation retained to help inform future preservation efforts. Any copying or reformatting of data for migration or conversion should be documented in the recordkeeping metadata.
- Preservation processes are carried out in accordance with relevant recognized recordkeeping, information and data management standards.
- Guidelines and procedures are issued and staffs are encouraged to adopt common usage rules to help standardize the application of the selected techniques across all public office systems.

Where records are migrated, converted, copied or reformatted, the success of the process must be verified and data integrity confirmed before the duplicate source records are destroyed. Any alteration or loss of functionality, structure, content or appearance that occurs as a result of preservation is fully documented in the recordkeeping metadata.

Thorough checking regimes are put in place following preservation to monitor record integrity and identify when further preservation treatments are required.

3.5.9 The Arkib Negara Malaysia approach to digital preservation

Preservation strategies involving migration, encapsulation and emulation of digital records are all effective and reasonable paths to maintain records that are active and regularly required for business and administrative purposes. These processes can maintain the integrity and accessibility of electronic records to ensure that developments in technology do not render electronic records inaccessible. Electronic records requiring long-term maintenance need to be actively managed in a planned, systematic and documented strategy.

The Arkib Negara Malaysia approach to the preservation of electronic records will be based on a combination of these techniques – conversion, encapsulation and emulation (see: ***Standards for the Management of Electronic Records*** - available from the Arkib Negara Malaysia).

Electronic records are converted or 'normalised' using archival data formats. The archival data formats use XML (eXtensible Markup Language) standard schemas. XML provides a standard syntax to identify parts of a document (known as elements), and a standard way (known as a schema) to describe the rules for how those elements can be linked together in a document.

Metadata is encapsulated within the preserved data object, and the whole package is stored in a digital repository. A special viewing tool makes the packages accessible using a form of emulation.

This approach allows the 'essence' of the record to be captured in a format that can be re-created as required and preserved over time. The concept of 'essence' is central to the Arkib Negara Malaysia digital preservation approach. 'Essence' refers to the essential characteristics that give a record it's meaning. These characteristics include the format, structure, content and context, as well as the overall 'look and feel' of a record.

This approach can be implemented regardless of the system from which the electronic records were derived. It works for records in any format for which an archival data format has been developed (referred to as XML normalisers). Current formats include email, proprietary word-processed documents, datasets, images and plain text.

The Arkib Negara Malaysia approach is compatible with migrating records across platforms – records do not need to be in their native formats (i.e. their original pre-migration data formats) in order to be converted to an archival data format. However, electronic records of archival value need to be converted to accessible data structures before their native formats become obsolete. Once original data formats are outmoded, there is a substantially increased risk that it may not be possible to normalize the records into archival data formats.

For more information on maintaining and preserving electronic records, and advice on developing electronic records preservation strategies, consult the Arkib Negara Malaysia.

3.6 Providing access to electronic records in agency custody

For agencies to meet their legislative obligations, their electronic records must remain accessible and usable, with the necessary infrastructure to meet public and official access demands. For long-term electronic records, it will be necessary to apply appropriate preservation strategies to enable continued access to the records. Public offices are also required to identify and retain appropriate metadata for electronic records.

To meet their access obligations, public offices need to:

- Identify which records are 25 years old and document how the age of records is calculated.

- Nominate staff able to liaise with the Archives, as well as officials and the public.
- Provide copies of, or electronic access to, electronic records.
- Keep a record of the access process.

3.6.1 Provision of secure access to electronic records

When providing access to electronic records, public offices should take appropriate precautions to ensure their security, integrity and authenticity. Like records on paper or any other medium, electronic records need to be protected from unauthorized alteration. As such, procedures should be established to supervise access to electronic records.

To avoid any compromise of the security, integrity and functioning of an public office's electronic record keeping system, the Archives recommends that access is not given to the live system, but rather to a clone or parallel system, or to copies of the records. Any sensitive or classified records should be appropriately expunged or made unavailable for access, in accordance with legislative requirements.

If public offices are unable to provide properly supervised access to electronic records, they should seek further advice from the Arkib Negara Malaysia.

3.6.2 Determining when a digital record can be open for access

For the purposes of determining the age of a particular digital record, the date of creation is the date from which to measure the age of the record. Updating an electronic record (e.g. saving, refreshing or migrating) does not impact on the 25-year countdown. In cases where the original transactions occurred on earlier electronic or manual systems, the date of first creation should be used rather than the date of transfer onto the current system.

Full and accurate metadata documenting dates for the creation, modification and preservation (e.g. migration or conversion) of electronic records will assist in determining the age and integrity of long-term electronic records.

Where there is doubt over the appropriate age determination of electronic records for access purposes, public offices should seek advice from the Arkib Negara Malaysia.

3.7 Disposing of Electronic Records

3.7.1 Obtaining approval for the disposal of electronic records

For standards and guidance on obtaining approval for the disposal of electronic records please see: *Electronic Records and the Akta Arkib Negara 2003* (available from the Arkib Negara Malaysia)

Disposition authorities which govern the removal of records from operational systems should be applied to records on a routine basis, in the course of normal business activity. No disposition action should take place without the assurance that the record is no longer required, that no work is outstanding and that no litigation is current or pending which would involve relying on the record as evidence.

Disposition action may encompass:

- Immediate physical destruction.
- Retention for a further period within the business unit.
- Transfer to an appropriate storage area under organizational control.
- Transfer to a storage area managed on behalf of the organization by an independent provider where appropriate contractual arrangements have been entered into.
- Transfer to an organizational archive.
- Transfer to the Arkib Negara Malaysia.

The following principles should govern the physical destruction of records:

- Destruction should always be authorized.
- Records should be destroyed as aggregates rather than selectively.
- Records pertaining to pending or actual litigation should not be destroyed with the class of records to which they relate.
- Authorized records destruction should be carried out in a way that preserves the confidentiality of any information they contain.
- When records are destroyed under authorization, all copies, including security copies, preservation copies and backup copies should be destroyed.

3.7.2 Methods of disposing of electronic records

There are three lawful ways to dispose of electronic records:

- Transfer electronic records of archival value to the Arkib Negara Malaysia once they are no longer required for agency business purposes.

- Transfer electronic records to another organization as a result of a change in government administrative arrangements, such as the privatization or redistribution of business functions.
- Destroy electronic records of temporary value once their minimum retention period has expired (most electronic records are of temporary value).

Some electronic records may need to be retained by the public office permanently. These records are not of archival value and, therefore, cannot be transferred to the Arkib Negara Malaysia. However, they must be preserved and remain accessible.

Metadata should be retained for electronic records that have been destroyed or transferred. More advice can be obtained from the Arkib Negara Malaysia.

3.7.3 Disposal in digital systems

Recordkeeping systems should be able to manage disposal with some degree of automation. Achieving this requires some forethought in relation to system design and the development of the public office's records disposal authority.

Automation is only possible when a disposal action is linked to an event that takes place within the system. For example, disposal may be triggered 10 years after a file is closed. The system has access to metadata about date of closure, and can dispose of the file automatically. Business rules can ensure that files are closed on a certain date (such as end of financial year), or when they reach a certain capacity.

In some cases, the system relies on the manual entry of metadata to trigger disposal. For example, if a superseded policy is to be disposed of ten years after the date on which it was superseded, then staff must mark it as superseded as soon as the new policy is developed. Such tasks may be easily overlooked, resulting in a backlog of records past their disposal date.

Coordination between records managers and systems designers will allow disposal of electronic records to be managed efficiently and with minimal intervention. Automating this process in systems with full recordkeeping functionality is the most effective way to demonstrate accountable disposal. Such systems will generate audit trails and metadata as evidence that records are managed in accordance with relevant disposal authorities.

3.7.4 Transferring electronic records to the Arkib Negara Malaysia

The Arkib Negara Malaysia is currently developing standards for the transfer of archival electronic records to its custody (see: ***Electronic Records and the Akta Arkib Negara 2003***). These will be based on existing procedures for the transfer of non-electronic records. More information can be obtained from the Arkib Negara Malaysia

3.7.5 Transferring electronic records between agencies

Periodic changes to the administrative arrangements of the Malaysian Government, such as the privatization of Malaysian government agencies or the redistribution of government functions between agencies, often create circumstances where government records are transferred from the controlling public office to another organization.

Transferring the custody or ownership of government records to an organization outside the Government of Malaysia must seek the approval of the National Archivist. Advice on transferring records between Malaysian government agencies can be obtained from the Arkib Negara Malaysia.

When electronic records are transferred from one public office to another, the relinquishing public office should transfer the electronic records, and their associated metadata, in data formats that are accessible and functional for the receiving public office. The receiving public office inherits the responsibility of managing, preserving, and providing access to the electronic records. The public office, therefore, needs to ensure that it receives adequate system documentation and metadata along with the electronic records.

If the relinquishing public office retains any copies of transferred records, the metadata for those copies should reflect the details of their transfer. Transferred files or containers should be closed, so that no more records can be added.

3.8 Destruction of electronic records

Most electronic records created and maintained by public offices are of temporary value and may be destroyed when they reach the minimum retention period specified within the public office's approved records disposal authority. Some records can be routinely destroyed in the normal course of business.

Destruction of electronic records involves ensuring that the record cannot be reconstructed. Most temporary electronic records will be required for relatively short retention periods and will not require preservation treatments – such as migration – to ensure their continued accessibility. Temporary electronic records that need to be retained for longer periods of time may need preservation treatments to ensure their accessibility until they can be destroyed. Given the vulnerability of electronic records, preservation treatments should usually be applied to records more than five years old.

3.8.1 Deletion is not destruction

In electronic systems, records are not destroyed when they are 'deleted'. What is destroyed is the pointer to the record (e.g. the file name and directory path) that tells the operating system where a particular piece of data is held on the medium.

The actual data objects are gradually overwritten in time by new data. However, until the data is completely overwritten there remains a possibility that the information can be retrieved. 'Deletion' does not meet the requirements for destruction of government records.

3.8.2 Methods of destroying electronic records

Disposal mechanisms should ensure the effective destruction of data. Such mechanisms include digital file shredding, degaussing (i.e. the process of demagnetizing magnetic media to erase recorded data) and physical destruction of storage media (e.g. pulverization, incineration or shredding). Reformatting may also be used as a method of destruction if it can be guaranteed that the process cannot be reversed.

To ensure the complete destruction of an electronic record, all extant copies should be located and destroyed. This includes removing and destroying copies contained in system backups and offsite storage.

More information on appropriate methods of destruction for electronic records and associated media formats can be obtained from the Arkib Negara Malaysia.

3.8.3 Retaining electronic records permanently within public offices

Some electronic records are identified for permanent retention within the public office. Maintaining these records indefinitely and accessibly is the responsibility of the public office. Public offices will determine their own approach to the long-term preservation of these electronic records, although the Arkib Negara Malaysia recommends its own electronic records preservation approach.

3.8.4 Retaining archival value electronic records in agency custody

In some circumstances, the Arkib Negara Malaysia may ask public offices to retain archival value electronic records rather than transfer them to the Archives. This will usually occur in cases where Archives staffs believe that the best prospect for preserving access to those records is to retain them within their original technological environment. Electronic records of archival value to be retained in the physical possession of agencies remain subject to the *Akta Arkib Negara 2003*

The Arkib Negara Malaysia will still be responsible for registering and describing the records in its control systems.

3.9 Documenting records management processes

Documentation describing records management processes and records systems should address legal, organizational and technical requirements. Authority for records management processes, such as classification, indexing, review and disposition of records, should be clearly stated.

Relevant legislation, standards and policies should be recorded, to determine requirements for practice, review, audit and testing of records management processes. Close attention should be paid to other information systems and policies, in use within the public office, to maintain integrity of the information management environment as a corporate entity.

All decisions on which records should be captured and how long records should be maintained should be clearly documented and retained. Decisions may be presented as a disposition authority. Formal documentation of the analysis or other assessment which results in decisions to capture and retain records should be prepared and submitted to senior management for approval. The documentation should contain details of business activities and the classes of records which result from each business activity, and specify their retention periods and disposition actions clearly and unambiguously. Events which activate or enable disposition actions should be clearly identified. Instructions for the transfer of records to alternative forms of storage (e.g. off-line or off-site storage) should be included. Where necessary, such documentation should be submitted to an external authorizing body, such as an archival authority, auditors, etc. for necessary approval.

4 Governance

This section address two perspectives on the governance required to manage electronic records effectively. The first pertains to the manner in which electronic records initiatives should be managed (i.e. by adopting a project management approach) while the second pertains to the management framework that should be in place to ensure that a sustainable electronic records management program is in place to address on an ongoing basis the business needs of the public offices they are designed to serve.

4.1 Governance of Electronic Records Initiatives

The steps that follow are in the form of a checklist of the factors that need to be considered in ensuring that the management of electronic records is accounted for in the planning, design, implementation, and review of systems supporting the programs and services of public offices.

4.1.1 Problem Definition

- Provide a clear identification of the 'problem' and a clear understanding of the record keeping requirements that must be respected by a system. What is the business or accountability problem that needs to be addressed?

    - In the 'structured' environment it might be that the absence of retention standards for controlling the length of time otherwise well-managed database records generated in a highly structured applications system is raising concerns about the system's compliance with certain laws and policies.
    - In the 'unstructured' environment it might be that the proliferation of e-mail messages and other electronic documents is causing concerns that valuable records of decision are being lost.
    - In the 'web' environment it might be that the absence of a relationship between a consultation draft of a policy posted onto the web and the records that document the process by which it was developed is raising concerns about the ability to provide evidence of how the consultation draft was developed.

- Identify a program manger who 'owns' the problem. A program manager must be in a position to say that if the initiative does not proceed then his or her program will be placed at risk. If the problem is only 'owned' by records management staff, systems developers, etc., then the effort to define the problem has not gone far enough.

- Obtain the commitment of senior management. Senior management must be completely aware of why an electronic record keeping initiative is required and be prepared to support the initiative throughout.

4.1.2 Cost Benefit-Analysis

- Conduct a comprehensive cost-benefit analysis to demonstrate why the initiative is required and why the outcome justifies the costs. The initiative could be:
    - To ensure that the design of an application system respects record keeping requirements.
    - To develop an electronic document and records management system (EDRMS) for the unstructured environment.
    - To enhance record keeping in a rapidly evolving web environment.
- Regardless, the benefits of the initiative must be weighed against the costs and must be expressed in terms of how the initiative can lead to cost avoidance, cost savings, risk reduction, and/or opportunity gain.
- Assess the element of risk both internally (internal policies, initiatives, etc. that require an enhancement to the record keeping environment) and externally (external policies, ordinances, initiatives, etc. that impose new and perhaps more stringent requirements for records management) and always within the context of the business function(s). More than factors such as cost savings or cost avoidance, the risk factor is often the major trigger for an electronic record keeping initiative.

4.1.3 Project Initiation

- Develop a project charter to guide the initiative. Such a charter should be as much about who is accountable for 'what' as it is about the objectives and methodology to be employed. In an initiative to enhance electronic record keeping in the 'web environment' it might be a program manager working with a web master and records management specialists. In the 'structured' environment it might be the systems development staff, database administrator, program manager, and records management specialists.
- Confirm an approval process for the various stages and deliverables of the initiative. Such a process should cover the mechanism for seeking approval for: the funding required to support the initiative; the standards, practices, and systems to be employed in carrying out the initiative; the 'go/no go' decisions that may be required as the initiative proceeds; and, the delivery of the final products of the initiative.
- Ensure the availability of the required project management skills to support the initiative. A project team needs to be assembled based on a clear set of objectives, methodology, deliverables, etc. Roles and responsibilities need to be assigned and reporting relationships confirmed.

- Establish a communications strategy to ensure that the initiative is understood clearly by those participating in the initiative and by those who may be its beneficiaries. Such a communications strategy needs to concentrate on clarification of the problem being solved, the strategy for addressing the problem, and what can be expected at the conclusion of the initiative (i.e. managing expectations).

4.1.4 Requirements

- Develop functional requirements to express what the system is required to do to support record keeping. User involvement in the requirements definition is critical if the design of the system is to be relevant.

    - In the structured environment the deliverable might be functional requirements for retention and disposition that can be incorporated into the overall functional requirements for an application system (e.g. licensing system, benefit delivery system, etc.).
    - In the unstructured environment, the functional requirements might be those supporting an EDRMS to address the management of e-mail and other electronic documents.
    - In the web environment the requirements might be those that are incorporated in the design of web content management systems that guide the posting of content onto the web or the systems that control transactions communicated via the Internet.

- Develop record keeping rules and other related rules and procedures to help guide users and others (e.g. systems developers, web masters, records registry staff) in creating, using, and maintaining electronic records and for managing functions such as retention and disposition, security, etc.

- Identify human resource requirements to ensure that the capacity is in place to manage the introduction of new tools and procedures and to ensure that those using them are equipped with the required knowledge, skills, and abilities. Change management requirements (training, briefings, orientation sessions plus strategies involving management leadership, mentoring, etc.) will also be important.

- Ensure the availability of facilities to support the record keeping aspects of new or modified systems. The space requirements for servers holding the repositories for electronic records, the specifications for back-up facilities, ‘archiving’ facilities, etc. need to be analyzed and expressed.

- Identify funding requirements based on the identification of the requirements described above.

4.1.5 Design

- Establish an architectural model that reflects the record keeping requirements. This will help to guide the further development of data models and other structural components of the system.

- Ensure that proposed solutions are in line with the evolution of the existing technology infrastructure. They must also account for the existing approach to record keeping in the paper environment and reflect how the electronic record keeping considerations will be reflected in the overall record-keeping environment.

- Establish performance measures to ensure that the specified record keeping requirements can be met and that they can continue to be met through time.

4.1.6 Implementation

- Design and resource a program of awareness setting and training to ensure that staff is able to create, use, and maintain electronic records to the desired effect.

- Design and implement a site 'readiness' study to ensure that the new or modified system is tailored to the work environment. The way people work, the way in which information flows through a given business process or given set of offices, the corporate culture of the organization, the existing records management practices (and the competencies of those involved), the existing technology specifications and configuration, and a host of other site specific components (e.g. bilingualism; security; etc.) will need to be understood.

- Analyze the existing work processes (e.g. business processes supported by applications systems; any workflow that may be identified in the 'unstructured' environment; content management processes in the 'web' environment) to determine how they can be improved, streamlined, or completely re-engineered in order to take maximum benefit of what a new or modified process can offer.

- Establish an understanding of the various ways in which information is:

  - Created:
    - Are criteria in place to guide where records need to be created?
    - What happens to records collected or received from others?
    - What are the attributes of the records once they have been created (re: ensuring their authenticity, etc.)?

- Used:
  - How do users access information?
  - What tools – such as a file plan, keywords, etc. – are used to find and retrieve records?
  - What kinds of records do they retrieve and why?
  - How are records transmitted or disseminated?
  - How are security classified records accessed and used?

- Preserved:
  - How are records classified?
  - How are retention standards established and where are records stored?
  - Who looks after the physical retention of records, their security, etc.? Have security, threat, and vulnerability assessments been undertaken for the personnel, network, physical facilities, transmission, and integrity of records?
  - Are vital records and security provisions being applied?
  - Are records retention and disposal schedules being applied?
  - What kinds of storage facilities and capacities will be required?

- Based on the site readiness analysis, establish a migration strategy to guide the transition from the existing situation to one that reflects the specified record keeping requirements. Issues ranging from technology and the application of business rules to training and change management will need to be addressed.

- Establish a prototype to confirm the extent to which proposed technology solutions as well as the rules established for records creation, use, and maintenance are viable and that they meet the functional requirements. Issues concerning scalability, costs, training and change management, etc. can also be identified through a prototype.

- Conduct an acceptance test to ensure that the prototype meets the functional and technical requirements.

- Develop a communications and rollout plan in line with the implementation of the system in order to ensure that users, stakeholders and others who have an interest in the system are kept aware of the implementation effort, its objectives, timetable, and outcomes.

- Conduct a user acceptance test to ensure that the new or modified system, once installed, meets the functional and technical requirements.

4.1.7 Maintenance

- Establish mechanisms to ensure that the new or modified system continues to meet performance requirements and the specified functional requirements (e.g. speed of records access and retrieval; application of retention standards; etc.).

- Develop change management procedures for the new or modified system and define the roles and responsibilities of those involved in managing the change management process.

- Develop procedures for monitoring the security and integrity of the new or modified system and especially the integrity of the repository holding the records.

- Establish mechanisms for supporting users of the system (i.e. help desks, etc.), especially as it relates to the creation, use and maintenance of electronic records.

- Develop processes for managing upgrades to the new or modified system (e.g. new versions of the software; new capabilities such as the addition of workflow software; etc.), maintaining the inter-operability of the system (i.e. according to pre-defined standards), and managing the life cycle of computer resources.

- Develop processes for migrating electronic records as required.

- Develop processes for anticipating emerging gaps in the competencies (i.e. knowledge, skills, abilities and training needs) of those using the system and those responsible for its management (e.g. records registry staff) and establish appropriate training and recruitment strategies.

4.1.8 Review and Evaluation (Quality Assurance)

- Establish performance standards and other evaluation criteria to ensure that the new or modified system meets the specified requirements.

- Define the roles and responsibilities of those responsible for the audits and evaluations. Identify who should be accountable for ensuring that the audits and evaluations are undertaken and identify the competencies (e.g. record keeping) required by those undertaking the audits to ensure that the audits are undertaken effectively and that the results will have meaning to those who will need to take corrective action.

- Evaluate the new or modified system for the extent to which it meets the requirements expressed at the outset of the project. The evaluation should cover the infrastructure of technical and functional requirements as well as human resources requirements and facilities.

The generic steps outlined above may be applied to address electronic record-keeping issues within any of the three computing environments generally supported by public offices.

4.2 Governance of Electronic Records Management Programs

4.2.1 Governance at the Government-wide level

The governance structure for the management of electronic records at the government-wide level is as follows:

ANM is responsible for:

- Providing interpretive advice on the *Akta Arkib Negara 2003*, particularly those provisions that touch on the handling of electronic records.
- Providing interpretive advice on these Guidelines.
- Helping public offices integrate electronic records management requirements into Government functions and information technology strategies and plans.
- Developing and promoting, in collaboration with relevant offices, e.g. MAMPU, a framework for development of tools, standards, guidelines and practices to support government-wide and institution-specific electronic records life cycle management initiatives.
- Representing and promoting the records management community and other relevant communities concerned with the management of electronic records, i.e. as required to develop and sustain the Records Manager's capacity that supports both this Guidelines and service delivery.
- Identifying, selecting, acquiring and preserving electronic records considered being of enduring value to Malaysia and providing access and usage facilities and services for the purpose of historical and evidential reference and research.
- Issuing Records Disposal Schedules to enable public offices to dispose of electronic records that no longer have operational value, by permitting their destruction (at the discretion of the Public Offices), or by requiring their transfer to ANM.
- Providing direction and consultation in electronic records life cycle management.
- Fostering smart partnerships directed to the advancement of electronic records management.
- Serving as a leader in building electronic records management capacity in the Government of Malaysia and as a credible resource on electronic records management.
- Promoting the establishment of national and regional networks to encourage collaboration among government and non-governmental organisations (NGOs) and to help position Malaysia as a leader in electronic records management.

Heads of Public Offices are responsible for:

- Ensuring the implementation of these guidelines and related policies and standards pertaining to the management of electronic records.
- Promoting a culture that values electronic records and their effective management.
- Allocating appropriate human and technological resources to support electronic records management.
- Designating a senior official to be accountable for implementing these guidelines and informing ANM of the appointment.

Senior officials are responsible for:

- Championing electronic records management.
- Coordinating the strategic planning, resource planning and implementation of electronic records management activities, including training and development for staff.
- Ensuring that electronic records management requirements are identified and addressed during program and system design.
- Ensuring that the effectiveness of the implementation of the guidelines is periodically assessed.
- Ensuring that electronic records management accountability frameworks and terms of reference are in place when electronic records are shared with other government institutions, other governments or non-governmental organisations (NGOs).

All public officers are responsible for:

- Applying electronic records management principles, standards and practices in the performance of their duties.
- Documenting their activities and decisions.
- Identifying and reporting requirements and issues to records managers and information technology personnel.

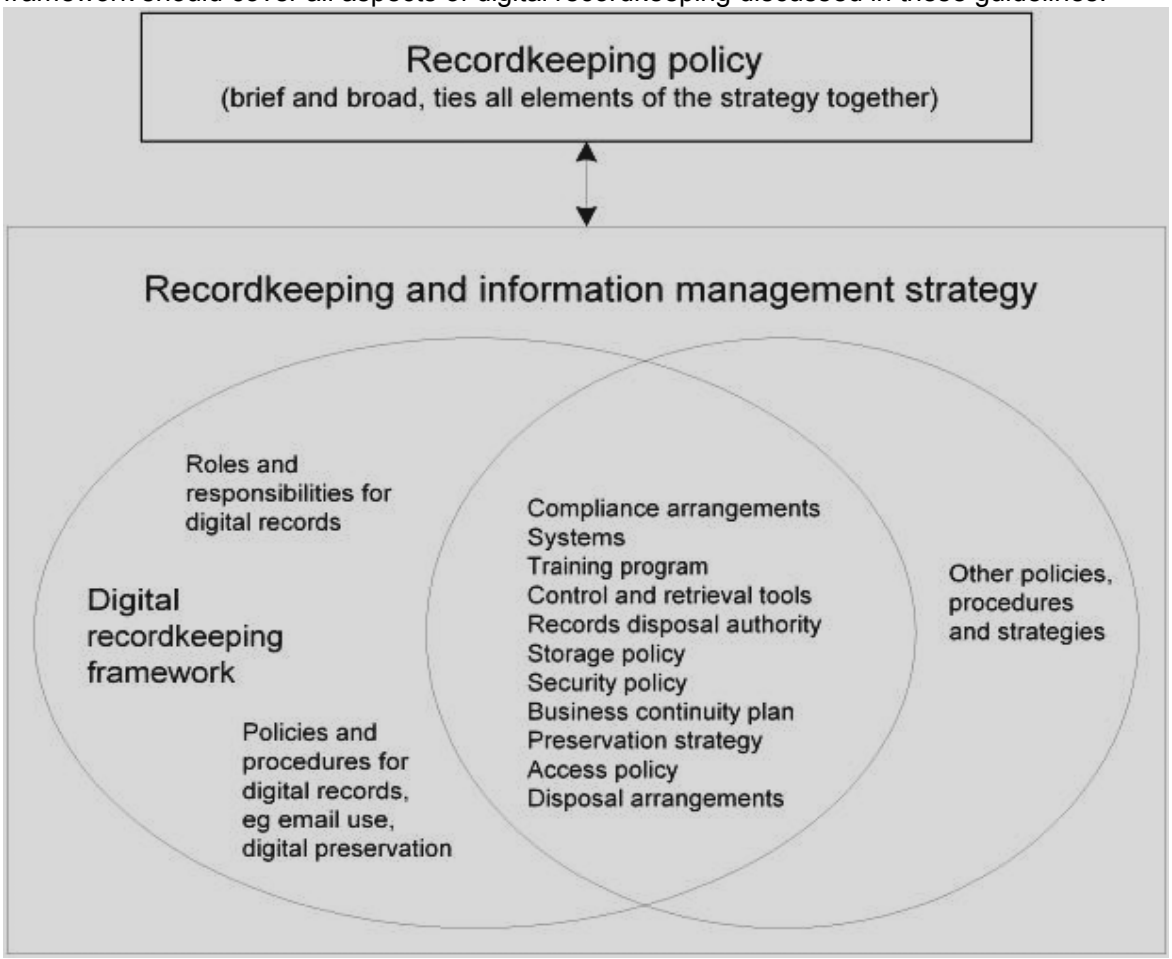
Records managers are responsible for:

- Providing electronic records management advice, support, necessary tools, policies, standards, guidelines and procedures consistent with direction provided by Arkib Negara Malaysia.
- Identifying requirements for information technology personnel to support the development and operation of information technology processes, systems, standards and tools.
- Assessing electronic records management resource and training requirements.
- Participating in the design, monitoring and updating of the policies, standards and practices and systems.

4.2.2 Governance at the level of the public office

Public offices should establish an electronic records management framework for the management of their electronic records. The framework should be integrated into the total recordkeeping and information management strategy for the public office and include all of the major players who will have a role in the management of electronic records. To this end, the governance structure for electronic records should integrate business process owners with legal advisors, IT support staff, and records management staff.

Public offices should ensure that an organization-wide recordkeeping policy is in place. Such a policy must relate to all agency records, regardless of format. An electronic recordkeeping framework covers a subset of a public office's records (i.e. its electronic records) and forms an integral part of the recordkeeping policy. An electronic recordkeeping framework incorporates arrangements for compliance with relevant standards and legislation, formal written policies, procedures and guidelines, identification of key roles and responsibilities, design and implementation of recordkeeping systems and user education and training. The framework should cover all aspects of digital recordkeeping discussed in these guidelines.



Public offices are encouraged to pursue a holistic approach to recordkeeping that is based on legal and business requirements, rather than record format. An electronic recordkeeping framework allows the management of electronic records to be integrated and consistent with the management of records in other formats.

Senior management recognition of electronic records as corporate assets, and commitment to their effective management, is essential to the success of an organization's electronic recordkeeping framework. Appropriate resources must be provided to develop and implement a sustainable organization-wide framework.

The scope and complexity of the framework an organization develops will depend on the organization's size, the complexity and level of risk of its business, resource availability, and the volume and type of electronic records created.

It is vital that an electronic recordkeeping framework ensures compliance with all relevant legislative requirements. The *Akta Arkib Negara 2003* requires the Arkib Negara Malaysia approval for the disposal of government records and allows for the provision of access to government records.

In addition to legislation that all public offices must abide by, public offices may need to abide by requirements contained in legislation specific to their business, in particular enabling legislation. Public offices that have already systematically identified their recordkeeping requirements will be able to make use of that analysis.

Public offices should also consider relevant standards such as those contained in, *Electronic Records and the Akta Arkib Negara 2003* (available from the Arkib Negara Malaysia).

There may also be relevant information technology (IT) standards for public offices to use when developing electronic recordkeeping solutions, e.g. data format standards and protocols like XML (eXtensible Markup Language), SGML (Standard Generalized Markup Language) and X.400 (an electronic message interchange protocol).

Policies and procedures for managing electronic records are an important element of the electronic recordkeeping framework. Policies define the public office's approach to managing electronic records and provide the necessary senior management authority for the implementation of the framework. Procedures outline how the policies will be implemented and provide clear instructions for their practical application. Where necessary, policies and procedures can be supplemented by guidelines to provide additional clarification and direction

The policies and procedures developed as part of an electronic recordkeeping framework should cover all aspects of electronic recordkeeping dealt with in these guidelines.

Policies, procedures and guidelines should be developed to suit the public office's size, complexity, corporate culture and structure. A small public office, for instance, may have a single policy covering the management of all digital records. Larger public offices may have multiple policies covering specific areas of digital recordkeeping, such as electronic messages, preservation of digital records, web-based digital records and digital records security.

The public office's IT environment should also be considered – for example, how many systems currently exist, potential for integration, what types of records are generated (e.g. data sets, spreadsheets, messages, images), whether staff work from the hard drive, shared folders or through an interface to multiple repositories. Considering these issues will help public offices choose a records management solution, and develop and implement effective policies and procedures.

Some issues that may be covered by policies, procedures and guidelines are:

- Setting up and managing the agency's electronic workspace.
- Developing and implementing document and directory naming conventions.
- Responsibilities for particular staff members or sections.
- Processes for capturing electronic records into corporate recordkeeping systems.
- Conditions of use for the electronic messaging system, including private use by staff.
- Implementing access controls and security measures.
- Coordinating document storage and disposal.
- Aligning IT management procedures with best practice digital recordkeeping.

Chief Secretaries are ultimately responsible for the management of records within their agencies. In most public offices, this responsibility will be delegated to an appropriate senior position, such as the Chief Information Officer (CIO).

The senior officer with this delegation should be familiar with the agency's IT and communication infrastructure. They should also understand the public office's recordkeeping requirements, the nature of its records and how to ensure their integrity over time. Records created on behalf of the public office by outsource providers remain the responsibility of the public office and should be included in the senior officer's responsibilities.

An important goal for the officer in this position is to promote collaboration between information management, records management, e-business, website management, IT and line of business staff. The skills, knowledge and experience of all areas are required for public offices to meet the challenges of electronic records. As such, responsibility for electronic records is shared across the organization. In particular, records managers play an important role in the development of recordkeeping and business information systems and in ensuring that records are created and maintained appropriately.

Responsibility for identifying corporate records created in the course of a public office's business activity is the responsibility of all agency staff. Staff may also be required to add metadata to records they use and create. With adequate training and clear and precise

policies, procedures and guidelines, staff should feel confident to identify records that need to be incorporated into the agency's recordkeeping systems.

Formal policies, procedures and guidelines to codify a public office's approach to electronic recordkeeping provide a solid foundation for managing electronic records. But the effectiveness of such a strategy will depend on the extent to which endorsed practices are actively adopted throughout an agency.

It is necessary to invest in staff education and training to encourage widespread adoption of electronic recordkeeping. Training and user education programs must be recognized as an integral, vital and ongoing component of a public office's electronic recordkeeping framework.

All agency staff, regardless of level, should be made aware of the legal requirements for public offices to create and maintain records, and should be educated about the electronic recordkeeping policies adopted by the public office. Staff with responsibility for electronic recordkeeping in a public office should be proactive in developing and delivering training to familiarize staff with the appropriate procedures for creating, managing and preserving electronic records.

Key topics that staff training programs should cover include:

- Importance of records.
- Which records are electronic records.
- Staff responsibilities.
- Practices for capturing electronic records into the agency's recordkeeping system.
- Security issues for electronic records.
- Capture of appropriate metadata.

To ensure that public office staffs are aware of their obligations and that agencies create and maintain full and accurate electronic records, active and sustained promotion of the importance of keeping electronic records is essential. Including electronic recordkeeping training in induction programs for new staff is central to the continued effectiveness of a public office's electronic records education and communication strategy.

5 Special Topics

5.1 Electronic Records and Business Continuity[7]

Loss of electronic records in a disaster can be crippling for a public office. Information is the lifeblood of modern business – communications, contracts, research data, strategic plans, policy advice, customer records, payments and receipts. Without records, business grinds to a halt, corporate memory is lost and public offices are vulnerable to a multitude of risks.

Data on digital storage devices can be more susceptible to damage through disaster than other record formats, such as paper or microforms. Relatively minor damage to digital storage devices can easily render all information contained on a storage device inaccessible.

Disasters that can affect electronic records include:

- Natural events such as earthquakes, cyclones, bushfires, floods and vermin plagues.
- Structural or building failure such as malfunctioning sprinklers, leaks in roofs, poor wiring and power surges.
- Industrial accidents such as nuclear or chemical spills.
- Technological disasters such as viruses and computer equipment failures.
- Criminal behaviour such as theft, arson, espionage, malicious computer hacking, vandalism, riots, terrorism and war; and
- Accidental loss through human error, unsuitable storage conditions (e.g. storage of magnetic media near electronic equipment generating strong magnetic fields) or by the natural decay of materials (e.g. corrosion of poor quality compact disks).

All electronic records and systems for which a public office is responsible should be incorporated into a business continuity plan. Appropriate disaster management arrangements for records created, and systems used, by outsource providers on behalf of the public office should also be provided for in contractual obligations.

5.1.1 Establishing a business continuity plan

The Arkib Negara encourages all public offices to develop, implement and maintain an effective business continuity plan to cover their electronic records and recordkeeping and business information systems. It is critical to plan and protect electronic records and business information systems from the risk of disaster, and to ensure the continuation of business in the event of a disaster.

[7] Based on guidance provided in *Digital Recordkeeping: Guidelines for Creating, Managing, and Preserving Digital Rec*ords, National Archives of Australia, consultation draft, May, 2004

Typically, a business continuity plan will comprise measures to prevent or minimize the impact of a disaster, protection strategies for vital records and disaster recovery and restoration procedures to be followed if a disaster occurs.

The key components of such a plan include:

- A general policy statement.
- Assignment of staff responsibilities, including contact details for emergency services staff and the public office disaster recovery team.
- Threat analysis identifying the most likely potential disasters.
- Steps for preparedness, response and recovery.
- Procedures for identification and declaration of a disaster situation.
- List of vital records, noting significant or vulnerable holdings, and associated location and control documentation.
- Clearly identified priorities for salvage.
- Details of equipment and materials available for use in disaster salvage and recovery
- Building plans identifying and addressing any potential site risks.
- Provisions for staff training and current awareness.
- Emergency funding and insurance arrangements.

Periodic monitoring and review of a public office's business continuity plan should be undertaken to ensure its continued viability and effectiveness.

5.1.2 Counter disaster strategies

Public offices should be proactive in matters of business continuity and ensure that appropriate procedures and practices are in place to minimize the risk of electronic records being lost or damaged as a result of disaster.

Before establishing a business continuity plan, public offices should undertake a risk analysis to determine the types of threats being faced, the likelihood of disasters occurring and the potential impact of the resulting loss of records. All reasonable risks affecting electronic records and business information systems should be identified, prioritized and assessed as part of the risk analysis, so that steps can be taken to determine appropriate counter disaster strategies.

Counter disaster strategies are measures devised and implemented to improve a public office's capacity to prevent, prepare for and respond to disasters. Implementation of these strategies is central to any business continuity plan.

The following represent the core counter disaster strategies for the protection of electronic records:

- Duplication and dispersal of vital electronic records.

- Transfer records of archival value to the Arkib Negara Malaysia as soon as they are no longer required for business needs.
- Regular and comprehensive system backups.
- Preservation of systems and application documentation and passwords.
- Secure storage facilities for digital devices, including fire and water resistant housings and appropriate environmental controls.
- High standards of systems security to prevent electronic records from being unlawfully altered or destroyed and to safeguard against computer viruses
- Procedures for managing critical work in progress which may not be backed up or which is located outside storage facilities.

5.1.3 System backups

Public offices should perform system-wide backups of all corporate data on a regular basis as a matter of routine operating procedure – with emphasis given to identifying and duplicating vital electronic records and those of archival value.

If it is not possible to separate vital records within a system (for example, in an electronic document and records management application), a backup should be made of the whole system. Metadata connected with these records should also be duplicated and maintained offsite with the copied records.

In order that system backups capture as much of a public office's business information as possible, counter disaster strategies should influence agency work processes (i.e. by encouraging the creation of policies to centralize business information).

Employees should be encouraged to work from network drives rather than their workstation hard drives, and discouraged from storing files on removable digital media. Where applicable, records should be captured into recordkeeping or business information systems as soon as practical. The digital recordkeeping framework should include guidelines discouraging the use of auto-archiving of emails and other user-controlled backup facilities. (See "*Managing Electronic Records in the Unstructured Environment*", available from the Arkib Negara Malaysia)

The frequency of backups, and the period they are retained, will be determined by the results of the public office's risk management assessment and organizational requirements.

System backups should be as comprehensive as possible and include information from all corporate directories and networked drives. In public offices where staffs are permitted to store corporate records to workstation hard drives, this data should be uploaded for backup. Backup procedures should also be established for electronic records stored offline on digital storage media.

5.2 Vital records

Vital records are records that are essential for the ongoing business of an organization, without which it could not continue to function effectively. These can include daily invoices through to the minutes of meetings of executive bodies. Vital records should be proactively identified.

Business continuity plans, including counter disaster and disaster recovery strategies, should give vital electronic records high priority. The most effective method of protecting vital electronic records is to duplicate the records and maintain the duplicates in secure offsite storage. The relative ease with which electronic records can be duplicated and the low cost of digital storage makes this strategy both effective and affordable.

Duplicate vital records and system backups should always be stored offsite at a sufficient distance from the originating office to be relatively secure from the effects of the same disaster. Storage facilities should be secure, have appropriate environmental controls and meet the requirements set out in Appendix 3.

In addition to storing duplicates of electronic records offsite, public offices will need to maintain duplicates of systems and application software and documentation, access codes, passwords, serial numbers and other information relevant for the reestablishment of the public office's computer systems. Ideally, the equipment necessary to access the records should also be stored offsite, or alternative sources of the equipment should be identified in the business continuity plan. It is not enough to preserve the electronic records. The capacity for the public office to access the records must also be preserved.

5.2.1 Electronic records of archival value

Every care should be taken to ensure that electronic records of archival value receive maximum protection. Counter disaster strategies should indicate that loss of archival value electronic records are not acceptable, based on risk analysis.

The best way to safeguard electronic records of archival value is to transfer them into the custody of the Arkib Negara Malaysia as soon as they are no longer required for immediate business needs.

Business continuity plans should include disaster recovery and restoration procedures to enable an agency to swiftly re-establish its business operations after a disaster.

Disaster recovery procedures should:

- Provide advice on recommended handling procedures and preservation techniques for damaged digital media.
- Enable the timely re-establishment of vital computer systems and critical data.
- Make arrangements for data integrity checking to ensure salvaged electronic records are intact.
- Ensure access to specialized data recovery services.
- Ensure that vital electronic records are restored as quickly as possible.

Recovery of electronic records should be given an appropriately high priority within an agency's business continuity plan, as delays in attending to the recovery of digital records can result in substantial loss of data. It is a good idea to identify requirements for point-in-time recovery (i.e. recovery of records as they existed at a particular point in time – e.g. just before the disaster), because reverting to an earlier backup will result in the loss of any records that were created in the interim period. While there are methods of recovering data from damaged or corrupted digital storage media, these processes can be very expensive and in many cases cannot retrieve all data lost.

One reason for major delays in re-establishing systems is the ready availability of replacement servers. Mission-critical applications should have failover servers (i.e. servers that automatically come online in the event of a problem with the primary server) and offsite standby servers to enable restoration as soon as possible. Disaster recovery procedures should be tested regularly.

5.2.2 Managing Encrypted Electronic Records[8]

Encrypting records by means of cryptographic key pairs ensures that documents, email messages, automated transactions and other digital objects remain confidential during transmission from one party to another. An electronic transaction may be encrypted by an individual on an ad hoc basis, or automatically by a computer system according to predetermined business rules.

The advantage of Public Key Infrastructure (PKI) in this situation is that parties do not need to be known to one another before transacting, as long as they are both subscribers within the government network. The public keys used to encrypt the transaction are accessible though known channels and there is no need to share private keys through a secured conduit.

[8] Based on guidance provided in *Digital Recordkeeping: Guidelines for Creating, Managing, and Preserving Digital Rec*ords, National Archives of Australia, consultation draft, May, 2004;also derived from guidance developed by the National Archives and Treasury Board Secretariat (Canada)

5.2.3 Record keeping for encrypted records

If electronic transactions are stored in an encrypted form, they may become inaccessible over time. The most likely reason is the unavailability of the private key needed for decryption. The Arkib Negara Malaysia therefore recommends that records not be stored in their encrypted form. Instead, once received, they should be decrypted and stored in an appropriately secure facility (preferably a tamper-proof recordkeeping system), together with the metadata, audit logs and digital certificate information required to establish an evidentiary trail and to provide contextual information.

If, as an additional protective measure, encryption is applied in a single transaction to cover all information stored on a secure server, public offices will need to ensure that the relevant encryption keys are securely managed over time. They must be updated when necessary, so that records contained on the server remain accessible. Keys should be available to authorized personnel only.

Public office procedures should ensure that successfully decrypted records are captured and stored within a suitable recordkeeping system. The system should meet applicable standards and address business and security needs, as well as privacy considerations. A record's capture and storage within the system should affirm its continuing authenticity, integrity, reliability and usability. This will negate the need for retaining the record in encrypted form.

Metadata that should be captured would include:

- The unique identifier or serial number of any digital certificate used in the transaction and its issuing authority.
- Date and time stamps of the encryption and decryption process.

Certain procedures will minimize the business risk of disputes. For example, if a public office receives an encrypted record that fails to decrypt, it should retain it together with the information detailed above. This will provide support in the event of factual disputes where the outcome may depend on proof of whose encryption applications were at fault.

Where a public office is the sender of the encrypted record, it should keep documentation that demonstrates the reliability and integrity of its encryption technologies. It should be able to show that the system routinely produces encrypted records that can be reliably and accurately decrypted without alteration.

To further establish a reliable audit and evidentiary trail relating to encrypted transactions, the public office should also retain unencrypted versions of records intended for later encryption and transmission, together with associated log files, recordkeeping metadata and appropriate digital certificate information.

5.2.4 Key management

As a general rule, keys and other material required to decrypt data should be accessible for the life of that data.

Where encryption is only used for confidentiality during transmission, there should be no need for a key management plan. Continued access to the encryption keys is unnecessary if the sending agency retains a record of the unencrypted transaction and the receiving agency retains the decrypted record of the transaction. However, both agencies should ensure that the records are captured with recordkeeping metadata relating to the encryption process.

If an agency decides to retain records in their encrypted form, then an ongoing key management plan is essential for enabling future access.

The records created or received using online security processes such as PKI, should be disposed of according to the business activity to which they pertain, It is important to note that unauthorized alteration of a record as evidenced by an unverifiable digital signature, or inability to decrypt an encrypted record, may constitute de facto destruction of a record.

5.2.5 Recordkeeping, security and information management framework

Authentication and encryption issues need to be addressed early and considered as part of an agency's overall recordkeeping, security and information management framework. Developing such a framework involves:

- Developing a policy and strategy for information management.
- Assessing and implementing recordkeeping and information systems to maintain required records.
- Identifying recordkeeping requirements.
- Assigning responsibilities.

5.2.6 Policy and strategy

To ensure the success of an online security program, especially when it involves the use of digital signatures and encryption, a strategy and companion policy for information resource management (including recordkeeping) should be developed.

Preferably, the strategy should be developed as part of the online security program, and be in place before implementation of the program occurs. Recordkeeping related to online security technology should be part of an agency's overall information management or recordkeeping policies.

Carefully thought-out strategy and policy documents are necessary, whether records will be captured and stored via an agency's existing recordkeeping system(s), or as part of a separate system.

5.2.7 Identify record keeping requirements

As well as managing records created by authentication and encryption processes, public offices need to know which records relating to their online security activities should be captured to support business needs, satisfy accountability requirements and meet general expectations of the broader community. Knowing recordkeeping requirements will facilitate the development of appropriate recordkeeping strategies and actions.

5.2.8 Assign responsibilities to records, business and IT managers

Online security is a complex web of software, hardware, technology providers, external service providers, personnel, policies, procedures and agreements. Each of these elements may impact on several areas within a public office that use or provide these services. To ensure that all recordkeeping requirements relating to online security are addressed in a comprehensive manner, it is essential that recordkeeping responsibilities are identified, assigned and promulgated across a public office.

Managers in the records, business or e-business, and IT areas will all have a role in the implementation and delivery of online security services. Establishing communication channels is a useful way of enabling information flow. Meetings should be held to ensure that questions and issues are addressed. Procedures can then be developed and disseminated to provide a measure of control.

Interoperability of systems is essential for ensuring optimum accessibility of information, and provides long-term cost savings to a public office. If an area responsible for implementing online security has established communication channels with other areas likely to have some responsibilities, the required specifications are more likely to be known and understood. Checklists can be developed to ensure and new systems purchased will have the desired characteristics. High-level schema can be written for existing systems that may not be fully interoperable.

Some of the questions that managers should be asking to ensure complete functionality are listed below.

Business manager

It is essential that the person responsible for overseeing the implementation of online security processes in an agency ensures adequate information flow to support areas, such as the IT and recordkeeping sections.

- Have communication channels been established with all relevant work areas?
- Are the proposed online security processes appropriate for the business activities to which they relate?
- Have all online security processes been tested to ensure they produce reliable electronic transactions, and the test results documented?
- Has the recordkeeping policy and accompanying strategy been integrated with existing policy, and distributed and approved by the business area?
- Do the business plan and risk assessments include recordkeeping considerations, such as evidential, legislative and accessibility requirements?
- Has a key management plan been developed, if necessary?
- Are relevant personnel accredited and security cleared where appropriate, including contracted staff?
- Are all systems suitably secured according to Government of Malaysia Government guidelines?
- Are contingency arrangements in place for a disruption in power, a security breach or a systems failure?
- Is there a policy in place for the ongoing monitoring and review of systems and strategies?

Records manager

If a public office uses digital certificates or performs online security processes, the records manager must ensure appropriate recordkeeping strategies for these transactions.

- Has a recordkeeping policy and accompanying strategy been developed and approved? Note that it should take account of the business needs of the agency's authentication and encryption activities.
- Have all recordkeeping requirements been identified, including legislation, standards and evidentiary requirements?
- Is there a disposal authority specifying retention requirement for electronic transactions?
- Is the recordkeeping system that captures and stores records of electronic transactions capable of maintaining the records appropriately, in a manner that preserves the content, structure and context of the records, and ensures their accessibility over time?
- Does the system maintain the authenticity of electronic transactions by, for example, capturing contextual metadata?

- Does the system allow for migration of records to new software platforms in a way that retains the authenticity and integrity of the records?
- Does the system have sufficient security controls? Do they meet Government of Malaysia guidelines?
- If a key management plan is necessary, has the recordkeeping section contributed to its development?

IT manager

The IT manager should be in close liaison with the business area responsible for implementing online security processes, as well as the recordkeeping section (or equivalent).

- Do existing systems meet stringent online security requirements?
- Are there sufficient personnel available to maintain the system to specifications?
- Does the system capture sufficient transaction-level detail as identified by the records or business manager?
- If more than one system is used, are they interoperable?
- Do systems meet Government of Malaysia standards for security, and are all logs and audit trails checked on a regular basis?
- Is there a contingency plan for physical security threats, such as loss of power? Does the plan include proper back-up and recovery procedures?
- If electronic transactions are not captured into a function-specific recordkeeping system, does the system capture and store records of electronic transactions? Is it capable of maintaining the records appropriately, in a manner that preserves the content, structure and context of the records, and ensures their ongoing accessibility and integrity?
- If a key management plan is necessary, has the IT area contributed to its development?

5.2.9 Records to be retained as national archives

Some records that result from electronic transactions processed within online security systems in the Malaysian Government may be appraised as being 'national archives' – that is, assessed as having continuing value according to criteria specified by the Arkib Negara Malaysia. These records will eventually be transferred to the National Archives and, subject to certain provisions, made available for public access after 25 years.

The Arkib Negara Malaysia custody policy is to accept any record deemed to have archival value, regardless of format, as soon as its business need has ceased. However, the Arkib Negara Malaysia will only accept electronic records created and used as part of online security processes in unencrypted or decrypted form. This will ensure that these records remain accessible, readable and retrievable. To preserve the quality of its collection, the Arkib Negara Malaysia also needs to ensure that records received into its care retain contextual information so that the integrity of the records is maintained.

Why? It is impossible for the Arkib Negara Malaysia to gain access to and store all the components of authentication schemes necessary to ensure their ongoing functionality. The Archives will be unable to re-validate digital signatures attached to records because it will not attempt to gain possession of the relevant public and private keys (or equivalent device).

Similarly, the Arkib Negara Malaysia will not have the ability to decrypt records. There are many different means by which a record may have been encrypted and it would not be possible to guarantee the ongoing functionality of each one – or even gain access to the various schemes.
If a record is transferred to the Arkib Negara Malaysia, it is unlikely that there will be a continuing business need for any attached digital signatures to remain functional.

However, a public office needs to make a risk management decision on whether it continues to support the key management plan for records that have been transferred to the Arkib Negara Malaysia. The agency may choose to capture appropriate recordkeeping metadata as sufficient proof that the digital signature was valid at the time of the transaction. On the other hand, the risk management process could require the agency to maintain the key management plan to provide access to the public key for the purpose of re-validation.

Unencrypted or decrypted records should be transferred together with the contextual information (e.g. encryption details such as the name of the CA or RA provider, the reference number of the digital certificate that contained the public key, and the date and time of the transaction).

Meeting the recordkeeping recommendations contained within these guidelines will ensure the accessibility, readability, integrity and completeness of electronic records created during online security processes, and ensure that records transferred as national archives will be well controlled and accompanied by appropriate metadata.

Records transferred to the custody of the Arkib Negara Malaysia will be stored in conditions that ensure their security and long-term preservation and accessibility.

Implementation Checklist

The intention of this checklist is to serve as a tool that public offices can use when planning to use authentication and encryption technologies.

Initial considerations

- Has your public office established the level of online security needed?
- Have online security processes been included in your public office's recordkeeping, security and information management framework?

Technology considerations

- Has your public office chosen the type of technology it will use, based on its security requirements and risk assessment?
- If your public office will use other forms of online security technology, have you investigated the privacy, user training, storage and access considerations related to particular forms of technology?

Recordkeeping considerations

- Has your public office developed a strategy and policy on information management and recordkeeping?
- Has your public office put recordkeeping and information systems in place to securely store and maintain its records?
- Does your public office know what records relating to its online security activities should be created and captured to meet legislative, business and community expectations?
- Does your public office produce documentation to prove the reliability and integrity of the encryption technologies it uses?
- Is your public office aware of the requirements imposed by Malaysian Government agencies with specific roles in the use of online security technology?
- Are staff with specific roles, such as the business manager, records manager and IT manager, aware of their responsibilities?
- Will recordkeeping metadata be used to document important details relating to the validation of a digital signature and the encryption of a record? If so, are procedures and systems in place to allow its capture and maintenance?
- Will your public office require a key management plan?
- Has your public office made arrangements to ensure that 'retain as national archives' records can be transferred to the Arkib Negara Malaysia in an unencrypted form, with appropriate contextual information?

5.3 Managing Electronic Records Created Outside Public Offices[9]

The continuing trend within the Malaysian Government of using external providers for government business activities raises a number of challenges for government accountability. Records relating to agency functions must be created, managed and disposed of in an accountable manner, even if the agency does not directly create, manage or dispose of them.

Contractual arrangements with external providers should:

- Explain that records remain the property of the Malaysian Government.

[9] Based on guidance provided in *Digital Recordkeeping: Guidelines for Creating, Managing, and Preserving Digital Rec*ords, National Archives of Australia, consultation draft, May, 2004

- Ensure the provider has the technical capability, for the duration of the contract, to manage electronic records and enable their viewing as required.
- Verify that the provider's systems will be compatible with those of the public office for the duration of the contract, in order to facilitate transfer of records back to the its public office.
- Specify that business continuity strategies are in place, including system backup procedures.
- Facilitate sentencing and disposal of records, including effective destruction where required.
- Specify how the provider can ensure the level of security required to safeguard the records.

These provisions will ensure that external providers can be held accountable for their actions, and enable public offices to meet their government and public obligations. Similar issues may arise where public offices exchange data or share integrated systems. Ownership and responsibility should be agreed, to determine who will capture and keep these records. Clear procedures and guidelines will ensure that vital records are retained.

The electronic recordkeeping framework should take into account electronic records created by external providers, or within shared systems. These records should be managed in accordance with public office policies.

For further advice on the recordkeeping issues involved in an outsourcing arrangement, consult with the Arkib Negara Malaysia.

Appendix 1

Key Concepts and Terms

In order to understand the concepts of "records" and "information" it is important to see them within a broader context of concepts such as "data", "knowledge", and even "wisdom". According to traditional information theory and in line with standards issued by the International Standards Organization (ISO),

- Data are the *representation* of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation or processing by human or automatic means;

- Information is the *meaning* given to data;

- Knowledge is the *understanding* given to information which results in *insight*;

- Wisdom is the *set of values* given to knowledge.

According to this framework, information does not exist as something tangible. It exists in peoples' minds as the meaning we give to data presented to us through a variety of means (on paper, on a screen, etc.). When people say they are managing information, they are really managing data or, to be more accurate, they are managing tangible surrogates of that meaning (text on a memo or in an e-mail; statistical information in a spreadsheet; a publication; etc.).

This is why it has been difficult to discuss what is meant by information management. How can one manage the "meaning" which resides in someone's mind? This is why terms such as "information holdings" or "information assets" or "recorded information" were introduced. It isn't the actual information or meaning that is being managed, it is the "representation", the "recorded information", the "holding", or the "asset" that is being managed. These concepts of asset, holding, etc. are "explicit" information as opposed to "tacit" information which is the information in one's mind based on acquired experience, etc. A NATO definition of information that attempts to address this concept is as follows:

> *Information: The intelligence or knowledge capable of being represented in forms suitable for communication, storage, or processing. (NATO – AAP-31)*

These concepts of "information", "explicit information", "information assets", etc. are congruous with the definitions of legal terms such as "record", "published material", "information holdings", etc. They essentially refer to any ***recorded*** information created, generated, collected, or received in the conduct of a government business activity.

According to an ISO definition (Information and Documentation - Records Management: ISO 15489, 2001), a 'record' is, "information created, received and maintained as evidence by an organization or person in pursuance of legal obligations or in the transaction of business." Based on this definition a record is something that has a purpose (i.e. it is not the residue of organizational activities). It is in existence because it needs to be there not only to serve as an instrument of accountability (i.e. evidence), but also as an authoritative, authentic, and reliable source of information (to make decisions, etc.). This definition comes much closer to the concept of records being an asset.

It follows that publications, by their very nature, have content, context and structure and that they exist because they have a purpose (e.g. to inform). It also follows that because they have a purpose, they should be considered an "asset". "Records" and "publications" or "published material" are assets and, similar to other assets such as financial and human resources, they are also assets that need to be managed.

The management of such assets is called "information management" (a convenient 'handle' for the 'management of 'recorded information' just as 'information object' is sometimes used as a convenient handle for record, publication, or any other discrete unit of recorded information).

A host of definitions of information management have been produced by private and public sector organizations as well as professional associations. The following definition developed by NATO is useful because it introduces the concept of information being 'exploited' - i.e. not just being administered through its life cycle.

> ***Information management:*** *The means through which an organization maximizes the efficiency with which it plans, collects, organizes, controls, disseminates, uses and disposes of its information, and through which it ensures that the value and potential value of that information is identified and exploited to the fullest extent. (Information Resource Management - Program Development, March 1998; NATO (AAP-31))*

Any model of information management must be *business and accountability driven*. In fact, information is such an integral component of the delivery of government programs and services that an understanding of information management as a concept cannot be obtained until one has first established an understanding of the business of the organization and the responsibilities of those within the organization.

The organization's information management activities and the IM infrastructure that is required to support these activities must be aligned with and contribute to the organization's business and accountability objectives. Figure 1 illustrates this fundamental concept as well as the key components of the IM infrastructure.

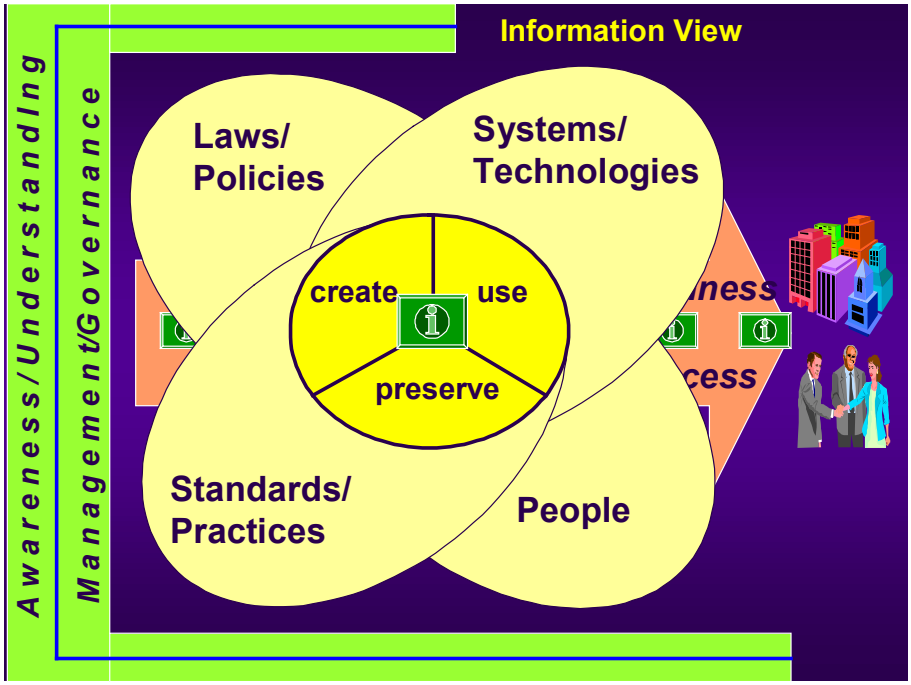


Figure 1: The IM Infrastructure

The organization's information management activities fall into three fundamental groups, namely:

- **Create**": activities *done to manifest* information products (i.e. bring it into existence) to support decision making, program delivery, and to meet accountability requirements. These activities include: create, generate, collect, receive, etc. The label given to this set of activities is "create".
- **Use**": activities *done with* information products to support decision making, program delivery, and to meet legal and accountability requirements. These activities include: transmit, exchange, access, retrieve, disseminate, share, exploit, etc. The label given to this set of activities is "use".
- **Preserve**": activities *done to* information products to ensure they are authentic, reliable, available, usable, and understandable for as long as required to support decision making, program delivery, and to meet other requirements. These activities include: organize, describe, classify, retain, protect, store, migrate, dispose, etc. The label given to this set of activities is "preserve".

These activities may be viewed at different levels;

- At the level of the individual **information object** (i.e. the briefing note);
- At the level of the **business process** (i.e. all of the information objects associated with the preparation and dissemination of the briefing note);
- At the level of the **organization unit** (i.e. all of the information objects for which a unit within the policy sector is responsible);
- At the level of the **function** (i.e. all of the information objects associated with the policy development function the responsibility for which might reside in one organizational area or be shared with multiple organizational entities);
- At the level of the **department** (i.e. all of the information objects under the control of the department);
- At the level of the involvement of **other external organizations** as active participants (i.e. all of the information objects associated with agricultural research policy as generated by the department, related government agencies, and foreign agencies) .

The activities are managed by an **infrastructure** of:

- **Laws and policies** that provide the mandate and direction for the creation, use and preservation of information (records, data, etc.)
- Appropriate **standards and practices** for the management of information over its life-cycle and in its many media and formats – creating, collecting, disseminating, identifying, organizing, filing, protecting, retaining, disposing;
- Effective technology-based **systems** to support information management activities and processes and which include business-centred information and technology architectures, applications and related systems standards and procedures;
- **People** (i.e. trained staff) to support information and knowledge management activities.

The infrastructure is required to ensure the effective management of the information activities described above and to ensure that they support the business and accountability requirements of the program or programs.

This infrastructure cannot exist in a vacuum. It must be supported by people who have an **awareness** and **understanding** of the value of information to their programs as sustained by a collaborative, information and knowledge sharing business culture within the organization. Awareness and ownership lead to greater ownership of information management and of business processes and outcomes.

But it needs more than this. The above infrastructure requires an effective **management and governance** framework that integrates and embeds information activities into all business processes, identifies IM responsibilities within the organization, provides leadership for IM, coordinates IM across the department, monitors and evaluates performance, etc. Such a framework extends across the organization:

- To the Chief Secretary or head of agency (who is normally accountable for the management of information just as he or she is accountable for the management of other resources);
- To the individual program managers and staff who are responsible for creating, using, and preserving the information they need to carry out their program responsibilities, and;
- To the specialists who are responsible for the policies, standards and practices, and systems which support the ability of program managers and staff to create, use and preserve the information they need.

Finally, the management and accountability framework as well as the design of the IM infrastructure itself must be guided by fundamental **principles** that reflect the values and requirements of an information-intensive organization operating in the public interest. These principles are:

- **Availability**: Information and data must be created, acquired and maintained so as to support and document important activities and decisions adequately;
- **Accessibility**: Information and data should be accessible to, and shared with, those who need to access it and have a right to do so and provided in a form that meets the users' needs;
- **Stewardship**: Personnel in the organization should be responsible for ensuring the accuracy, authenticity, relevance, timeliness and reliability of their information resources;
- **Creation and Retention**: Information should be created, acquired and retained only for valid government business, legal, policy, accountability and archival needs;
- **Privacy and Security**: The security of information should be protected to ensure privacy, confidentiality and information integrity, consistent with business, legal and policy requirements;

The accountability framework must be supported by policies, audit standards, and methods to measure the extent to which the IM infrastructure is (or is not) implemented and operating effectively.

In many organizations, the design of the **IM infrastructure** may not be consistent across the entire organization. This is because the nature and design of the business processes as well as the computing environments supporting the business processes will often vary in accordance with the nature of the organizations' business functions. In order to more clearly understand the IM implications of what is often a highly complex landscape of business processes and computing environments the following categorization has been established.

> **'Unstructured' Environment** where business processes and workflow are not clearly defined, the user has relative autonomy over what information is created, sent and stored (e.g. as e-mail and attachments) and accountability for the management of information (including information in 'records') is unclear. This is the world of e-mail and other electronic documents that are generated without the benefit of structured work processes or rules of the road. Typically it is a user driven world where the user has autonomy concerning what gets created, how it is transmitted and how it is stored and otherwise managed. The absence of workflow within which records/documents (regardless of their physical form) can be placed in a context presents a substantial challenge from a recordkeeping perspective. Electronic recordkeeping solutions tend to be derived from the world of paper based records management.
>
> **'Structured' Environment** where business processes are typically highly structured, well-established tools and techniques are employed to develop application systems supporting the processes, and accountability for the design, development and maintenance of systems (including the integrity of the data generated in the systems) has been assigned. This is the 'systems' world where the processes for carrying out the business of the public office have been heavily structured, where accountability for the design, development and maintenance of the systems supporting these processes has been assigned and where the accuracy and reliability of the 'data' generated and managed in these systems must be ensured in order to support the overall integrity of the systems. The management of electronic records should work best in this kind of environment because a platform of accountability, defined work processes and business rules and a codified approach to systems and data design has been established. It doesn't always succeed (which is why there are issues - often related to retention, disposition and long-term preservation - connected with this environment) but at least a framework of policies, standards and practices, systems and technologies and people exists to manage the processes and the multiple forms of information (including records) generated by the processes. Usually, in the absence of an adequate understanding of the record keeping

issues in this environment, solutions tend to be derived from the world of systems development and data management.

'Web' Environment where work processes are generally associated with the 'publication' and 'communication' of information (though this is changing rapidly with the advent of E-Government initiatives) and the role of the web master is dominant. This is a rapidly evolving environment. It is the world of 'web content' in which, in the earliest stages of web site evolution, organizations find themselves 'publishing' content onto the web (ergo the issues in this environment tend to be derived from the world of communications, publishing, marketing and library services). But in this era of E-Government, they are also finding themselves managing records that have emerged from defined work processes such as those connected with the development of policy (e.g. the preparation of various drafts of a consultation document placed on the web site or the handling of enquiries placed via the e-mail facility featured on most web sites – similar to 'correspondence management'). Pursuant to the agenda established for many e-government initiatives, many organizations are evolving even further by turning their web sites into gateways or portals in order to support on-line transaction processing (e.g. e-filing of tax returns). In the early stages of web site evolution, any record keeping-related issues are expressed as content management issues (e.g. authenticity, reliability, integrity, security, etc.) and solutions tend to be derived from the publishing/communications world. In later stages both the issues and the solutions may be more closely aligned with the worlds of records management, data management and applications systems development. Over the longer term, the 'web' environment will reflect the convergence of multiple business processes, multiple disciplines and multiple (increasingly integrated) solutions.

The categorization described above is not based on the nature of the records. It is based on the nature of the business processes and the computing environments that support those processes. The fact that e-mail is so challenging to manage in the 'unstructured' environment is because the work processes associated with e-mail are often ill defined or non-existent. It is the processes that are 'unstructured', not the records[10]. Conversely, the records of those applying for a license may be managed more effectively simply because the processes in such a 'structured' environment are well-defined and the rules for what records are kept, what they look like, where they are kept and for how long, can be built into the design of the business process.

In summary, the **business process environments** (unstructured, 'structured', 'web') reflect different types of **business processes** that support **business functions** supporting the goals and activities of a given organization. The business processes

[10] In fact, all records are structured regardless of the environment in which they were generated! An e-mail message containing 'to' and 'from' fields (as well as other structured fields) is a 'structured' document. Even a scrap of paper with some text on it may be structured in that its boundaries are the scrap of paper with jagged edges, the free following un-justified text, etc.

generate information objects (i.e. they are created, used and preserved to support the business of the organization) that must be managed by an **IM infrastructure** comprising policies, standards and practices, systems and technologies and people.

Appendix 2

Definitions

Terms	Definitions
Acquisition	The acquisition of records by the Archives by way of transfer, purchase, donation, bequest, gift, etc.
Appraisal	A process by which decisions on the retention, disposal or transfer of records are taken
Appraisal Agreement	A legal document that binds Arkib and the Agency with respect to the details of the records appraisal process
Archival value	The determination in appraisal that records are worthy of permanent preservation by an archival institution.
Archival Records	A record, or record series, which has been designated by the State Archivist to have historical administrative, fiscal, legal, intrinsic, evidential, or informational value. At the end of the Retention Period, such records should be transferred to the Archives for preservation.
Audit	The process of reviewing, verifying, evaluating and reporting by an independent person(s) on the adequacy of a unit of analysis against a predetermined set of criteria. In the case of a business systems analysis project, the criteria for the audit derive from implementation objectives.
Authenticity	The quality of being authentic, or entitled to acceptance
Capture	Capturing the record within the electronic environment involves management of the interface between the record keeping system and the applications, such as word processors or e-mail clients, which are used to create or receive records. Systemic capture requires both a technical interface and a set of rules or procedures which govern its behaviour and successful application within the organization
Classified records	Means public records which are classified as official secrets within the meaning of the *Official Secrets Act 1972 [Act 88].*
Creation	Individual records are created in order to carry out defined business activities. Within this context records are created when they are created by authorized individuals, using forms specified for the activity to which the record relates. A body of records is created when individual records are created (as indicated above), appropriately filed with received records (e.g., incoming correspondence), and related to other records (e.g., through a file classification plan).

Terms	Definitions
Custody	A reproduction of the contents of an original document, which is not the official file copy of the agency. Copies are usually identified by their function, i.e., action copy, reading file copy, tickler file copy, etc. In most instances, copies will have a shorter retention than the official file copy of a record series
Context	The organizational, functional, and operational circumstances in which documentary material is created and/or received and used.
Disposition Schedule	A schedule for deletion or destruction of records from record-keeping systems, the migration or transmission of records between record-keeping systems, and the transfer of custody or ownership of records to an archive or repository for permanent preservation. Disposal actions (including destruction) should always be documented, preferably by the record-keeping system itself
Electronic records	Computerized versions of traditional paper records created and kept by agencies. Sources of electronic records range from desktop applications such as Word, Excel, and e-mail, to corporate applications such as financial systems, HR systems and corporate databases.
e-File plan	File plan are used to organize and categorize information holdings. A file plan consists of a collection of different types of objects, which have names like Prefix, File, Section, Folder, Volume, Primary, Secondary etc. This allows records to be efficiently located based on the categories of information to which they belong.
File	• In the records management sense, a file (or folder) groups associated records in a logical structure that shows the position of one record in relation to others. A file will have an identifying title or label, and other characteristics, and will be part of a wider structure which reflects the business activities of the organisation. By means of the file/folder, a whole group of records can be managed together, and the same actions can be taken on all records in that group at the same time. • In the computer systems sense, a file refers to a discrete object which can be stored as a separate entity on disk storage; for example, a word-processed document, a spreadsheet, an e-mail message. In this sense, it equates more closely to the idea of a part within a record in the records management sense. • In this guidance, file is always used in the records management sense, unless otherwise specified.
Metadata	Metadata is structured data about data. Metadata is descriptive information about an object or resource whether it is physical or electronic. Metadata can be manually created or derived automatically using software. In an e-mail the to, from, date, subject etc would be the metadata. In a Word document the summary portion of properties would be the metadata. (U Virginia)

Terms	Definitions
Non Formal records	• Non-work material, i.e. literally 'personal'. • Personal work-related material, e.g. the usual light-hearted banter that fills the E-mail. • Trivial work-related material, e.g. routine housekeeping information such as the time and place for meetings, administrative details. • Incomplete material, e.g. papers or memos begun with enthusiasm but for one reason or another never completed or shown to anyone else. • Drafts not sent for comment, approval or to file, i.e. as with the above category, the material was seen by no one except the creator;. it was not communicated to anyone else or to file. • Copies of material sent from elsewhere for information only, i.e. the equivalent of paper circularised information: the material originates elsewhere and is not meant to result in an action on the part of the recipient. This does not include reports or data received as part of the organisation's business. • Electronic bulletin board material not addressed to the recipient personally or to their agency, as well as information down-loaded from libraries, databases, etc. • Copies of letters, etc used as templates for other documents, where the documents themselves have been filed, e.g. a standard memo kept for later modification. • copies of all material printed out and filed on an organised multi-user filing system, or filed electronically under agreement with ANM and; • electronic copies of all paper material already recommended for destruction under a disposal authority approved by ANM, i.e. if the paper equivalent has already been deemed to be of no permanent value.
Operation Records	A record that continued to be used by the agency for as long as it is needed
Public office	An office of the Federal Government or the Government of any State or an office of any local authority, statutory authority or Government enterprise.
Record (PRO 3.13 – 3.15)	• In the records management sense a record is the result of an activity or transaction, and may result in more than one physical object; for example, a spreadsheet which is accompanied by a text commentary, or an e-mail message with several attachments. The record is made meaningful by the co-ordination of these parts, and will lose some of its sense with the loss of one or more of the objects of which it is constituted. • In the computer systems sense, a record refers to a tightly bound grouping of data which describes a distinct entity, usually in a database or other structured system. • In this guidance, record is always used in the records management sense, unless otherwise specified. Section 2 of the Procedures volume deals with types and sources of records.

Terms	Definitions
Records	Materials in written or other form setting out facts or events or otherwise recording information. Includes papers, documents, registers, printed materials, books, maps, plans, drawings, photographs, microfilms, cinematograph films, sounds recordings, electronically produced records regardless of physical form or characteristics and any copy thereof. Public records means records officially received or produced by any public office for the conduct of its affairs or by any public officer or employee of a public office in the course of his official duties and includes the records of any Government enterprise and also includes all records which, on the coming into operation of this Act, are in the custody or under the control of the ANM of Malaysia established under the *Akta Arkib Negara 2003 1966*[Act 511]
Recordkeeping	The act or process of creating, maintaining, and disposing of records
Records Management	The efficient and effective management and control of the creation, maintenance, use, and disposal of records, files, and forms
Records Lifecycle	An archival concept that describes the lifespan of a record, from its creation or receipt to its final disposition. The records lifecycle is divided into the following stages or phases: creation/receipt, maintenance and use, retirement, final disposition, and continuing use
Repository	A place where archived records are preserved and made available for consultation
Retention Period	The length of time a given records series must be kept, expressed as a time period (e.g., four years), an event or action (e.g., audit), or a combination (e.g., six months after audit)
Retrieve	Getting back or recovering an electronic record or object from on-line, near-line, or off-line storage
Public records	See “Records.”
Structured	The physical or logical form of a documentary material or a set of documentary material

Terms	Definitions
Unstructured	Environment in which business processes and workflow are not clearly defined, the user has relative autonomy over what information is created, sent and stored (e.g. as e-mail and attachments) and accountability for recordkeeping is unclear. This is the world of e-mail and other electronic documents that are generated without the benefit of structured work processes or rules of the road. Typically it is a user driven world where the user has autonomy concerning what gets created, how it is transmitted and how it is stored and otherwise managed. The absence of workflow within which records/documents (regardless of their physical form) can be placed in a context presents a substantial challenge from a recordkeeping perspective. Electronic recordkeeping solutions tend to be derived from the world of paper based records management
Vital Records	Records without which an organisation could not continue to operate – i.e., those containing information needed to re-establish the organisation in the event of a disaster. Vital records are those that protect the assets and interests of the organisation as well as those of its clients and shareholders.
Web	Rapidly evolving environment in which, in the earliest stages of web site evolution, organizations find themselves 'publishing' content onto the web (ergo the issues in this environment tend to be derived from the world of communications, publishing, marketing and library services). But in this era of E-Government, they are also finding themselves managing information that has emerged from defined work processes such as those connected with the development of policy (e.g. the preparation of various drafts of a consultation document placed on the web site or the handling of enquiries placed via the e-mail facility featured on most web sites – similar to 'correspondence management'). Pursuant to the E-Government agendas established by many countries around the world, many are evolving even further by turning their web sites into gateways or portals in order to support on-line transaction processing (e.g. e-filing of tax returns)

Appendix 3

Managing Storage Media for Electronic Records

Selection of suitable media

The storage media chosen should be stable and fully compatible with the information retrieval system. Floppy disks should not be used to store e-mail records of long-term or permanent value.

Media labelling

The removable storage media should be identifiable by external labels with sufficient information about the media and records stored therein. Such identification information may include:

- Unique identifier of each tape/disk/disc.
- Name of the organizational unit responsible for the record.
- Descriptive title of the content.
- Date of creation.
- Security grading.
- Type of copy, i.e. master or backup.
- Operating environment, i.e. hardware and operating software.
- Name and version number of the software which creates the attachment.
- Manufacture date of the storage medium.
- Storage location.

Label contents of the media should be written before attaching the labels to magnetic and optical media. Soft felt-tip markers should be used to prepare the label contents to avoid debris and scratches.

Handling and storage of the media

The storage media should be handled by their edges and kept away from dust, smoke, heat, direct sunlight and strong magnetic field. Magnetic and optical media should be shelved in an upright, vertical position to prevent warping of containers. They should be kept in protective containers when not in use.

Electronic records of long-term or permanent value are best preserved in an appropriate storage environment with 24-hour air conditioning and controlled temperature and humidity at 18°C ± 2°C and RH 40% ± 5% respectively. For assistance in storing long-term or permanent e-mail records, Departments should contact the National Archives.

Departments should provide proper access control and fire fighting equipment and facilities in the storage area to protect the physical security of the media.

At present, the physical life span of electronic media is still debatable and technology obsolescence also complicates the preservation of electronic records. Departments should thus develop strategies for system migration and implement a proper copying cycle to transfer their e-mail records, especially those requiring long-term or permanent retention, from old media to new media (e.g. from old CD-ROM to new CD-ROM). Normally the interval for media copying should be set for less than 10 years.

Frequent checking of the media

Departments should check samples of the tapes/disks/discs at regular intervals to ensure the integrity of the media and see that the information is retrievable. Should any signs of deterioration be found, the records should be copied to tested tapes/disks/discs as soon as possible.

At present, the physical life span of electronic media is still debatable and technology obsolescence also complicates the preservation of electronic records. Departments should thus develop strategies for system migration and implement a proper copying cycle to transfer their e-mail records, especially those requiring long-term or permanent retention, from old media to new media (e.g. from old CD-ROM to new CD-ROM). Normally the interval for media copying should be set for less than 10 years.

Types of magnetic media

The term 'magnetic media' is used to describe any record format where information is recorded and retrieved in the form of a magnetic signal.

The common types of magnetic media are:

- magnetic tape, including audio cassettes and reel-to-reel tapes, videotapes, computer tapes both on open reels and in cassettes, and tapes used in digital recording processes;
- magnetic hard disks; and
- magnetic floppy disks or diskettes.

Composition of magnetic media

Magnetic tape consists of a carrier of plastic film coated with a matrix containing magnetisable particles. The matrix also contains a plastic or resin binder, and other ingredients such as lubricants and fungicides. Sometimes the tape is coated on the reverse side with an antistatic material to reduce the build-up of static charges, and to improve its winding capability.

Magnetic hard disks have a metallic base, usually of aluminum. The base is coated on both sides with a matrix similar to that of magnetic tape.

Disk packs, which have a wide application in computing, consist of a number of hard disks stacked together around a central spindle. They require a special recording and playback system with many pairs of read/write heads.

Floppy disks and diskettes consist of a plastic base with a magnetic matrix on one or both sides. They are enclosed in a rigid, plastic protective jacket, which does not easily flex or bend. A slot in the jacket allows the read and write head to make contact with the disk.

Deterioration of magnetic media

All materials degrade over time. We cannot control this inevitable deterioration, but we can slow it down.

Some materials are inherently prone to deterioration, while others will only significantly degrade if they are stored in poor environmental conditions.

Below are examples of the types of deterioration to which magnetic media are prone:

- The tape carrier can become brittle and easily broken. The matrix on tapes and disks can deteriorate and subsequently flake off the base.
- The particles which retain the coded information in the magnetic layer can become unstable, leading to a gradual loss of signal quality and eventually to total information loss.
- Print-through, which is the transfer of a signal from one loop of tape onto an adjacent loop, occurs when tapes are stored for long periods without being played or exercised. The result is poor signal quality.
- Fluctuation and high levels of temperature and humidity may cause the magnetic and base layers to separate, or cause adjacent layers in a reel of tape to block together. High temperatures may also weaken the magnetic signal, and ultimately completely demagnetize the magnetic layer.
- Tapes are particularly susceptible to mould because pockets of air trapped in the windings can create microclimates which will support mould growth.
- Exposure of the magnetic layer to dust particles, dirt, grease and chemical pollutants can promote moisture condensation and oxidative deterioration. These contaminants also interfere with the contact between the playback head and the tape, resulting in a weakening of the recording or playback signal.

Magnetic fields

Because magnetic media store information by the alignment of magnetic particles, even a small external magnetic field can cause information loss on a tape or disk if it is in close proximity for long enough. Magnetic fields can be generated by items such as fridge magnets, magnetic screwdrivers and most machines with electric motors.

The degree of risk depends on several main factors: how close the media is to the source of the field; the strength of the field; and the duration of exposure. The effect of a magnetic field decreases with distance. This means that running a vacuum cleaner past the shelves will probably not cause any damage, whereas storing tapes or disks close to a large electrical generator could result in serious loss.

Handling

Always handle magnetic media as carefully as possible.

Pick up magnetic tapes by their protective cases; do not touch the tape.

Wear lint-free gloves, or ensure that hands are clean and dry.

Support open-reel tapes by the hub during handling and transportation.

Disks should never be flexed, bent or picked up by the oval slot in their jackets, or by the centre hole of the disk.

Labeling should be in ink rather than pencil, as graphite dust from the pencil could interfere with the reading of the disk or tape. Once applied, labels should not be written on, and should only be attached to a protective case, rather than directly onto the magnetic tape or disk.

Only remove items from their protective packaging for immediate use, and always return them to their containers directly after use.

Cassettes and tapes should be wound to the end of one side after use. They should never be left in a partly wound state for any length of time, and the use of the 'pause' mode should be avoided.

Special care should be taken when moving magnetic media. Ensure that the media are not bumped or dropped, and that they are properly packed in custom-made transportation canisters. For the transport of large quantities or important material, consult freight and courier companies who specialize in magnetic media.

Protective packaging

Paper and cardboard enclosures are unsuitable for the storage of magnetic media, as they tend to generate dust.

Tapes should be stored in cases made of non-magnetic material, preferably an inert plastic such as polypropylene. Polyvinylchloride (PVC) is unsuitable because it contains substances that may be damaging. Cases should have fittings to hold the tapes in position by the hub. They should be strong enough to protect the cassettes from physical damage, and they should close tightly to keep out dust particles.

Reels or cores used for winding tapes should be clean and free from cracks or sharp edges. There should be slots in the flanges of the reels to prevent bubbles of air from being trapped between the layers of tape on the reel. Reels should be made of aluminum or a stable plastic such as polypropylene (not PVC).

Floppy disks and diskettes should be stored in protective envelopes that have a non-abrasive surface and are resistant to the build-up of static electricity. Special envelopes are widely available and are suitable for this purpose.

Storage requirements

Qualified staff should check storage areas to ensure the absence of magnets or magnetic fields that exceed acceptable limits. Walls, floors, wiring, and all storage and electrical equipment within the area must also be checked.

Storage areas should be free from potential sources of dust, such as typewriters, paper shredders, printers and carpet. Measures, such as the installation of an air lock, or the maintenance of positive internal air pressure, should also be taken to prevent dust entering from the outside.

Magnetic media should ideally be stored in closed metal cabinets to provide extra protection against heat and dust. However, if adequate environmental controls are in place, storage on open shelves and racks is acceptable. All storage equipment should be sturdy, allow tapes and disks to be stored vertically, and most importantly, be electrically grounded.

Storage environment

Magnetic media should be stored in a temperature and relative humidity range of 18-20°C, and 35-40%, respectively. Under these conditions the natural deterioration of the objects can be slowed. In some instances deterioration can be further slowed by storage under lower temperatures. It is important that these environmental levels are stable. Mould will start to grow at around 60% relative humidity, and if the humidity fluctuates more than 10% in 24 hours or the temperature is too high, the items will be subjected to physical stresses that will accelerate their deterioration.

Exposure to ultraviolet (UV) light will also hasten degradation. Fluorescent tubes with UV-filters should be used wherever possible in storage areas, and turned off when not in use. UV light can be easily measured with a light meter, and levels should not exceed 75μW/lumen. An ideal storage area would have no windows, but if windows are present they should be covered with curtains or blinds.

Cleanliness is very important in records storage areas, both for the sake of the records, and from an occupational health and safety perspective. Never allow food or drink to be taken into a records storage area, and ensure the area is cleaned regularly. Insects and rodents, once attracted to a records storage area by food, may begin to eat the records.

Dust, heat and moisture can cause irreversible damage to magnetic media. Therefore storage areas should be fitted with special alarm systems, such as VESDA (Very Early Smoke Detection Alarm). Use of these systems can provide much earlier warnings of fire or high dust levels than conventional detection systems, and also minimize the need for large amounts of water to enter the storage area in the case of a fire. Fire detection and

suppression technology is rapidly developing, and advice should be sought at the time the system is required to ensure the best method is employed.

Maintenance

The information held on magnetic media can only be processed or read by mechanical means, therefore it is essential that equipment is maintained in good condition: the use of poorly maintained equipment can actually cause damage to records. The heads, disk drive and tape drive elements of playback and recording equipment should be cleaned regularly according to manufacturers' recommendations.

Some tape manufacturers also recommend the exercising of tapes to improve their life span. Problems, such as creases or folds in the tape, may build up as the tape pack sits in storage. Exercising can reduce the stresses that cause these problems and may also reduce the danger of print-through.

Exercising involves winding the tape slowly through its entire length at playback speed, without stopping. The process should be carried out in the same environmental conditions in which the tapes are to be stored. Tapes which are to be moved to a different environment for exercising should be allowed a period of 24 hours to acclimatize to the new environment before exercising them. It is generally recommended that exercising be carried out at least every three years.

Reformatting and data migration

To minimize deterioration due to handling and use, copies of important and frequently used tapes should be made for reference purposes. Ideally, a preservation master copy, a duplicating copy and a reference copy should be produced, and clearly labeled as such. As a disaster preparedness measure, the preservation master copy should be stored in a different location to the others. The duplicating copy may be used to produce further reference copies when required.

Long-term preservation of magnetic media is affected by two major factors: the intrinsic instability of the media; and the likelihood of the hardware required to read the media becoming unavailable. Even if tapes or disks made today are in excellent condition in 30 years time, the machines required to play them will almost certainly have been superseded long before, and for all practical purposes the records will be unusable. Beta format videotapes are a good example of this problem. Once very common, they have now been entirely superseded by VHS format tapes and it will soon be very difficult to view a Beta video.

The main prospect for long-term retention of the information held on magnetic media seems to be in regular copying or data migration, thus maintaining a good quality signal

that can be read using available equipment. Copying can either be to fresh tape or disk, or to some other machine-readable format such as CD-ROM.

Copying to analog tape will involve some loss of signal quality at every copying stage. This may be significant after as few as two or three copies. The problem may be overcome by copying to a digital format such as digital tape (DAT for audio tapes) or optical disk. The tape used for digital recording is no more permanent than the tape used for analog recordings but the information can be copied many times without a significant loss of quality. The problem does not arise with computer tapes as they are already recorded digitally.

Digital recording hardware is expensive. To minimize costs you can record initially on analog tape and then transfer to a digital medium for archiving. You should consider whether the information will need to remain on magnetic media permanently, or whether a paper or microfilm format would be a better way of retaining the information. Paper-based records and microfilm will always last longer than magnetic records stored in the same conditions.