ELECTRONIC RECORDS MANAGEMENT SYSTEM (ERMS)

SYSTEM SPECIFICATIONS FOR PUBLIC OFFICES

CONTENTS

1. INTRODUCTION

Good management of records and information is fundamental to a well-functioning organisation since it supports business activity and provides a basis for efficient service delivery. It also provides the mechanism whereby both the private and public sectors can account for their decisions and actions. Records provide evidence for the public to confirm or claim their public rights and entitlements, as well as providing individuals with evidence to justify government decisions and a mechanism whereby they can have trust in private enterprise. Moreover, good records management is simply good business practice.

Records management systems facilitate:
- efficiency, by making information readily available when needed for decision-making and operational activities;
- sound use of financial resources, by allowing timely disposal of non-current records;
- accountability, by enabling the creation of a complete and authoritative record of official activities;
- compliance, by demonstrating that legal requirements have been met; and
- risk mitigation, by managing the risks associated with illegal loss or destruction of records, and from inappropriate or unauthorised access to records.

1.1 Background

This document is part of the Electronic Records Management System - System Specification for Public Offices. The original document was developed by the National Archives of Malaysia under the First Phase of the e-SPARK project. This new version (version 2) of the System Specifications has adapted and incorporated all the recommendations from the International Council on Archives, Principles and Functional Requirements for Records in Electronic Office Environments Project in which the National Archives of Malaysia also participated in. This project was aimed at producing globally harmonized principles and functional requirements for software which is used to create and manage electronic records in office environments.

This document focuses on the creation and management of electronic records. It has been arranged with many headings and sub headings for ease of understanding and carries clear descriptions as outlined in the International Council on Archives, Principles and Functional Requirements for Records in Electronic Office Environments – Module 2: Guidelines and Functional Requirements for Electronic Records Management Systems, 2008. It is intended for use by the public and the private sector organizations that wish to introduce, develop and implement Electronic Records Management System, or to assess the Electronic Records Management System capability they currently have in place. This is established to ensure that the electronic records (e-records) generated by the public sector (or the

private sector) can be preserved while maintaining its authenticity, reliability, integrity, usability, and accessibility at any time.

1.2   Scope

The scope of this system specification is limited to products that are usually termed 'electronic records management systems'. It does not seek to set requirements for records still in use within business systems. Digital objects created by email, word processing, spreadsheet and imaging applications (such as text documents, and still and moving images), where they are identified to be of business value, should be managed within electronic records management systems that meet the functional requirements in this system specification. Records managed by an electronic records management system may be stored on a variety of different media formats, and may be managed in hybrid record aggregations that include both electronic and non-electronic elements.

This system specification does not attempt to include requirements that are not specific to, or necessary for, records management, for example, general system management and design requirements. Nor does it include requirements common to all software applications, such as the performance, scalability and usability of the application. Given the target audience of this document, it also assumes a level of knowledge about developing design specifications, procurement and evaluation processes, and therefore these issues are not covered in this specification. Although not included in this specification's requirements, the importance of non-records management functional requirements for records management systems is recognised through their inclusion in the high-level model outlined in Section 2.3: Overview of functional requirements.

1.3   Purpose

This specification articulates a set of functional requirements for electronic records management systems. These requirements apply to records irrespective of the media in which they were created and stored. They are intended to:

- explain processes and requirements for identifying and managing records in electronic records management systems;
- develop requirements for records management functionality to be included in a design specification when building, upgrading or purchasing electronic records management systems software;
- inform records management functional requirements in the selection of commercially available electronic records management systems; and
- review the records management functionality or assess compliance of existing electronic records management systems.

This specification is a revised version of the original document which was developed by the National Archives of Malaysia under the First Phase of the

e-SPARK project. This version has adapted and incorporated recommendations from the International Council on Archives, Principles and Functional Requirements for Records in Electronic Office Environments : Module 2 - Guidelines and Functional Requirements for Electronic Records Management Systems and is designed to:

- assist organisations to improve electronic records management practices;
- reduce the duplication of effort and associated costs in identifying minimum level of records management functionality for electronic records management systems; and
- establish greater standardisation of records management requirements for software vendors across different jurisdictions.

1.4 Audience

The primary audience for this document is:

- **by potential ERMS users:** as a basis for preparing an invitation to tender;
- **by ERMS users:** as a basis for auditing or checking an existing ERMS;
- **by training organizations:** as a reference document for preparing records management training, and as course material;
- **by academic institutions:** as a teaching resource;
- **by ERMS suppliers and developers:** to guide product development by highlighting functionality required;
- **by record management service providers:** to guide the nature of the services to be provided;
- **by potential users of outsourced record management services:** as an aid in specifying the services to be procured.

This document has minimised the usage of specific records management terminology. Where the use of such terminology is necessary, definitions can be found in the Glossary at Appendix 2.

1.5 Related standards

The requirements in this system specifications are aligned with the records management principles in ISO 15489 Information and Documentation – Records Management – Part 1: General, which sets out the records management requirements that also apply when records are captured and managed within electronic records management systems.

The reference metadata standard for these requirements is ISO 23081 – 1: 2006, Information and Documentation – Records Management Processes – Metadata for Records, Part 1 – Principles. The high-level metadata element set found in ISO/TS 23081 – 2: 2007, Information and Documentation – Records Management Processes – Metadata for Records, Part 2 – Conceptual and Implementation Issues provides the basis for the requirements in this system specifications.

The requirements presented in this system specification are core, high-level and generic requirements for records. Readers seeking guidance in other areas of software functionality not addressed in this Module can refer to other more detailed specifications such as US DoD 5015.2 and MoReq2.

1.6 Terminology

Many of the terms used in this document have differing definitions across disciplines. For example, the term 'archive' may mean a storage of little-used data in a database to an IT audience, whereas it means the retention of fixed appraised information no longer retained for current business use within the records management discipline. It is therefore important that this document is read in conjunction with the Glossary at Appendix A. A number of the central concepts used in this document are also outlined below, to avoid misinterpretation:

• **Records** – information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business.[1] They provide evidence of business transactions and can exist in any format.

• **Records management** – the control of the creation, receipt, maintenance, use and disposal of records in accordance with professional and international standards of practice. Records management is distinct from document management, which is typically concerned with the provision of access, collaborative working and version control of documents, rather than the management of authenticity, reliability, integrity and usability over time.

• **Electronic records management systems** (commonly referred to as EDRMS or ERMS) – systems specifically designed to manage the maintenance and disposition of records. They maintain the content, context, structure and links between records to enable their accessibility and support their value as evidence. Electronic records management systems are distinguished from business systems, for the purpose of this document, because their primary function is the management of records.

• **Business systems** – automated systems that create or manage data about an organisation's activities (for the purpose of this document). They include applications whose primary purpose is to facilitate transactions between an organisational unit and its customers, for example, an e-commerce system client-relationship management system, purpose-built or customised database, and finance or human resources systems. Business systems typically contain dynamic data that is commonly subject to constant updates (timely), able to be transformed (manipulable) and holds current data (non- redundant). For the purpose of this document, business systems exclude electronic records management systems.

---

[1] International Standard on Records Management, ISO 15489.

• **System** – use of the term 'system' in this document refers to a computer or IT system. This is in contrast to the records management understanding of the term, which encompasses the broader aspects of people, policies, procedures and practices. While the focus of this Module is primarily electronic records management systems software, organisations will need to pay attention to wider aspects of records management frameworks, policies and tools to ensure records can be appropriately managed. For example, fundamental   records management tools, such as disposition authorities and information security classifications, must be in place and operate within an established records management culture within the organisation. A system may comprise more than one application and include plug-ins

• **Records management metadata** – an inextricable part of records management, serving a variety of functions and purposes. In a records management context, metadata is defined as data describing the context, content and structure of records and their management through time (ISO 15489 – 1: 2001, 3.12). As such, metadata is structured or semi-structured information that enables the creation, registration, classification, access, preservation and disposition of records through time and within and across domains. Records management metadata can be used to identify, authenticate and contextualise records and the people, processes and systems that create, manage, maintain and use them, and the policies that govern them. Initially, metadata defines the record at its point of capture, fixing the record into its business context and establishing management control over it. During the existence of records or their aggregates, new layers of metadata will be added because of new roles in other business or usage contexts. This means that metadata continues to accrue information relating to the context of the records management and the business processes in which the records are used, and to structural changes to the record or its appearance.

Metadata can be sourced or re-used by multiple systems and for multiple purposes. Metadata applied to records during their active life may also continue to apply when the records cease to be required for current business purposes but are retained for ongoing research or other values. The purpose of records management metadata is to ensure authenticity, reliability, usability and integrity over time, and to enable the management and understanding of information objects, whether these are physical, analogue or electronic. However, metadata also needs to be managed as a record or as a component of a record.

Records management has always involved the management of metadata. However, the electronic environment requires a different expression of traditional requirements and different mechanisms for identifying, capturing, attributing and using metadata. In the electronic environment, authoritative records are those accompanied by metadata defining their critical characteristics. These characteristics must be explicitly documented rather than being implicit, as in some paper-based processes.

2 GUIDELINES

2.1 What are records and why are they important?

Records are a valuable business asset. One of the key ways organisations are held accountable for their actions is through evidence of business transactions in the form of records. Records are 'information created, received, and maintained as evidence and information, by an organisation or person, in pursuance of legal obligations or in the transaction of business'. [2] They must be retained for a period of time that is in line with an authorised retention schedule or disposition authority, sometimes referred to as a 'disposition'.

A record is not just a collection of data, but is the consequence or product of an event and therefore linked to business activities. A distinguishing feature of records is that their content must exist in a fixed form, that is, be a fixed representation of the business transaction. Managing records in business systems, which contain data that is frequently updated and dynamic, is particularly challenging and may provide a rationale for implementing a separate electronic records management system. Records comprise not only content but also information about the context and structure of the record. Records management metadata 'identifies, authenticates and contextualises records and the people, processes and systems that create, manage, maintain and use them and the policies that govern them.' [3] It allows records to be located, rendered and understood in a meaningful way. ISO/TS 23081 – 2 provides a generic statement of records management metadata elements. Organisations may also have jurisdiction-specific elements sets to which they must adhere.

An appropriately managed record will provide a basis for:
- transparent, informed and quality decision-making and planning;
- an information resource that can be used to demonstrate and account for organisational activities; and
- consistency, continuity and efficiency in administration and management.

The International Standard on Records Management, ISO 15489, provides best- practice guidance on how records should be managed to ensure they are authentic, reliable, complete, unaltered and usable. Organisations that do not employ an electronic records management system may risk loss of key evidence of their business activities, thereby resulting in a lack of corporate memory, inefficiency and an inability to meet accountability and legislative requirements. The risks of not implementing an electronic records management system are:
- failure to meet legislative and regulatory requirements;

---

[2] International Standard on Records Management, ISO 15489

[3] International Standard on Information and Documentation – Records Management Processes – Metadata for Records, ISO 23081.

- embarrassment to your chief executive, the government and/or private individuals, especially if inability to manage information competently is highlighted in the media;
- poor strategic planning and poor decisions based on inaccurate information;
- business critical information not accessible for the conduct of business, dispute resolution, legal challenge or evidential purposes;
- loss of credibility, lowered public confidence, or financial or legislative penalties through inability to produce records or provide evidence of business activity when required in a timely manner;
- inability to provide evidence of the organisation's activities or undertakings with external agencies, clients or contractors;
- inconsistent and inefficient conduct of business;
- inability to exploit organisational information and knowledge to full potential;
- unlawful disposal of records and inability to fully exploit corporate knowledge and data;
- duplication of effort, and poor resource and asset management;
- reduced capability of demonstrating good performance and any increased efficiencies or improved service delivery; and
- organisational embarrassment and damage to reputation.

The benefits of good recordkeeping include:
- protection and support in litigation, including the management of risks associated with the existence or lack of evidence of organisational activity;
- protection of the interests of the organisation and the rights of employees, clients, and present and future stakeholders;
- improved security of business records and robust management of commercial-in-confidence, personally sensitive or confidential information;
- the ability to deliver services in an efficient and consistent manner;
- ability to support current and future research and development activities;
- improved comprehensiveness and reliability of corporate memory;
- availability of relevant business activity records when required to support well-informed decision-making and policy development;
- reduced risk of data loss or accidental destruction of records;
- reliable performance measurement of business outputs;
- increased public and/or client confidence in the integrity of an organisation's activities; and
- identification of vital records for disaster planning, so that organisations can continue to function in the event of severe disruption.

Authoritative and credible recordkeeping is an essential component of good governance and for underpinning reliable and consistent business practice and service delivery.

2.2 Characteristics of electronic records and electronic records management systems

Once records have been created, they must be managed and maintained for as long as required to ensure they have the following characteristics:[4]

- **Authenticity** – the record can be proven to be what it purports to be, to have been created or sent by the person that created or sent it, and to have been created or sent at the time it is purported to have occurred.

- **Reliability** – the record can be trusted as a full and accurate representation of the transaction(s) to which they attest, and can be depended on in the course of subsequent transactions.

- **Integrity** – the record is complete and unaltered, and protected against unauthorised alteration. This characteristic is also referred to as 'inviolability'.

- **Usability** – the record can be located, retrieved, preserved and interpreted.

Typically, electronic records management systems have the following attributes that seek to ensure these characteristics are maintained:

- **Creating records in context** – electronic records management systems enable organisations to capture evidence of their business activity. This involves identifying a set of electronic information to serve as the evidential record comprising both content and context. So, in order for information to have the capability of functioning as a record, it is necessary to augment that content information with additional data (that is, metadata) that places it in the context of the business operations and computing environment in which it was created.

- **Managing and maintaining records** – electronic records have to be actively managed as evidence of business activity, and to maintain their authenticity, reliability, integrity and usability. Maintenance of this evidence, as records, is necessary for operational viability and accountability of the organisation.

- **Maintaining records for as long as they are required** – records must be retained for a period of time that is in accordance with authorised legislative and jurisdictional requirements. Decisions about

---

[4] These are taken from ISO 15489.1 Records Management, Section 7.2 Characteristics of records.

how long records must be retained are defined in disposition/disposal policies and rules. There will be some records that must be retained permanently while others will be required to be retained for varying periods or have a maximum retention period (for example, for privacy or data-protection legislative purposes).

Records have to be able to be disposed of in a managed, systematic and auditable way. A hallmark of appropriate records management is the retention and appropriate disposition of records according to specified rules as stated in Section 27 of National Archives Act 2003.

Systems need to be able to delete records in a systematic, auditable and accountable way in line with operational and juridical requirements. Organisations will need to meet the policies and procedures of their local jurisdictional authority for identifying, retaining and disposing of records.

- **Records management metadata can be configured** – to be meaningful as evidence of a business process, records must be linked to the context of their creation and use. To do this, the record must be associated with metadata about the business context in a classification structure. In addition to this 'classification' metadata, other metadata that should be captured at the point of creation includes:

  - record identifier (as specified in the e-file plan);
  - date of creation;
  - creator/author/person responsible; and
  - the business being conducted
  - etc

  Much of this information can be automatically generated. In this Specification, integration of metadata for managing records is addressed at a relatively high level. Rather than specifically detailing every metadata element required, the functional requirements set instead provides broad references to the need to have functionality that is capable of creating, capturing and maintaining adequate metadata elements. It is expected that each organisation will capture records management metadata in line with an identified records management metadata standard, in accordance with organisational and/or jurisdictional requirements, and/or be consistent with ISO 23081 – 1: 2006, Information and Documentation – Records Management Processes – Metadata for Records, Part 1 – Principles; and ISO/TS 23081 – 2: 2007, Information and Documentation – Records Management Processes – Metadata for Records, Part 2 – Conceptual and Implementation Issues.

- **Records can be reassigned or reclassified, closed and if required, duplicated and extracted** – the identification of needs for records should establish at what point in the process a record should be created. Any further Processes that happen to the record after this

point must result in the creation of a new record or the recorded augmentation/versioning of the existing record, rather than alteration to it. This means that content and metadata that need to be kept to record previous decisions or processes cannot be overwritten, but that new content or metadata can be added.

It is important to ensure that the system is not 'locked down' to such an extent that simple mistakes (such as mistyping a name) cannot be corrected – although permission for changes may be restricted to a system administrator or prevented by the system in exceptional circumstances, such as pending legal action.

- **Reports can be undertaken** – on records and the management thereof.

- **Security processes can be put in place** – normal systems controls over access and security support the maintenance of authenticity, reliability, integrity and usability, and therefore should be appropriately documented.

A risk assessment can inform business decisions as to how rigorous the controls need to be. For example, in a high-risk environment, it may be necessary to prove exactly what happened, when and by whom. This links to systems permissions and audit logging, to prove that approved actions are undertaken by authorised users. User requirements should be assigned at appropriate levels of access by an administrator.

Table 1: System levels of access

User	Any person with permission to access the electronic records management system. That is, anyone who creates, receives, reviews and/or uses records stored in the system. This is the standard level of access that most employees of an organisation will possess.
Authorised user	A user with special access permissions that allow additional access to, and/or control over, records contained in the electronic records management system. Authorised users may in some instances be assigned permissions to undertake tasks similar to those of the system administrator, such as the ability to close and re-open records, create extracts of records and edit record metadata. The powers assigned to authorised users will vary depending on the business needs of the organisation and the level of responsibility allotted to the authorised user
Records administrator (or records manager)	A system administrator, usually the records manager, with designated responsibility for configuring, monitoring and managing the electronic records management system content and its use.
System administrator (IT)	A person with responsibility for assigning and removing the permissions allocated to users and authorised users.

2.2.1 Supporting import, export and interoperability

The ability to import and export records, and interoperability with other systems, is frequently required functionality. Records may need to be exported to other organisations in the event of mergers or government re-organisational changes.

Many records may need to be retained for longer than the lifespan of the software system itself, and therefore there is a need to be able to export records when transitioning to a new electronic records management system. There may also be a need to import records from business systems, particularly in collaborative business environments.

For ease of import and export, use of open formats and industry standards will increase levels of interoperability and reduce the cost and difficulty of any import/export process.

This functionality must be addressed at the planning stages as part of the business requirements.

2.2.2 Authentication, encryption and technological protection measures

These issues have an impact on the reliability of records issue. Electronic records management systems must allow records to be effectively managed when they have been subject to technological protection measures, electronic signatures and electronic watermarks (digital rights management). They should give particular consideration to the ongoing maintenance of records that have been subject to encryption and digital signatures. While encryption and digital signatures have a valuable role to play in ensuring the authenticity and integrity of records in transmission, they also present risks to the ongoing usability of the record as decryption keys and public keys for digital signatures may expire while the record is still required. For this reason, storing records in encrypted form is not recommended. Metadata can record the encryption and decryption processes and attest to the successful decryption of records.

If digital signatures are used as a means of protecting the authenticity and integrity of records, key management must be considered. Information about the digital signature and its validation should be recorded within the metadata.

2.3 Overview of functional requirements

This section identifies and briefly describes the functional requirements using a high- level model that clusters the requirements to highlight their inter-relationships (Figure 1). The model is primarily intended to provide an overview for readers who are not records management professionals.

Requirements for the long-term preservation of records, requirements common to all software applications and non-records management

functionality are not detailed in this Specification, but are indicated in the high-level model (solid grey shading). Potential integration points with IT architecture and other software applications are shown in the model as system inputs.

Individual requirements in the Functional requirements are grouped according to the clusters in the high-level model:

- create
- maintain
- disseminate
- administer

Figure 1: Model of high-level functional requirements for electronic records management

DESIGN
- Ease of use
- Scalability / performance
- System availability
- Interoperability

Non Records management functionality

PRE-REQUISUITES / APPRAISAL AGREEMENT
- E- file plan
- Retention schedule
  (See Appendix 1)

2.3.1 CREATE
- Capture
- Identification
- Classification

2.3.2 MAINTAIN
- Controls and security
- Hybrid records
- Retention, migration and disposal
- Long-term preservation

2.3.3 USE, ACCESS AND DISSEMINATION
- Search, retrieve and render

2.3.4 ADMINISTER (RECORDS MAINTAINANCE MANAGEMENT)
- Administrative functions

INPUTS
- Desktop applications
- Workflows
- Websites
- Databases
- Imaging systems
- Business applications
- Email
- Others ★

Notes:
- Solid grey shading indicates functionality not detailed in Functional requirements.
- This model depicts the functional requirements that are the components of electronic records management systems. It does not depict the sequence of work processes that electronic records management systems perform.

★ According to the National Archives Acts, records also include 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, sound recordings, electronically produced records regardless of physical form or characteristics and any copy.

2.3.1 Create

Capture

Electronic records management systems uniquely capture, classify and identify records to ensure that their content, structure and context of creation are fixed in time and space. These records management processes facilitate the making of complete, authentic and usable records. There should be functionality to create a new record by reusing the content, structure and context of records once captured. While version/document control is beyond the scope of this specification it may also provide some of this functionality.

Records aggregations

Aggregations of electronic records are accumulations of related electronic record entities that, when combined, may exist at a level above that of a singular electronic record object, for example, a file. Aggregations represent relationships that exist between related electronic records and the system or environment in which they were created, and are recorded in their metadata links and/or other associations. These aggregations are typically controlled within a classification scheme in an electronic records management system. Electronic records management systems may contain aggregations of records, records that are not aggregated, or both. Records aggregations structure related electronic records and support their management and usability. They may be at more than one level, and may have multiple relationships within separate aggregations.

Aggregations of electronic records may reflect relationships such as shared characteristics or attributes, or the existence of sequential relationships between related electronic records. The nature of the relationship between the electronic records of a particular aggregation will vary depending on factors such as their purpose and structure, and the content and format of the records themselves.

For example, an aggregation of electronic records may collectively constitute a narrative of events (that is, a series of connected business transactions), in which the records may have a sequential relationship. Any such sequential relationship between electronic records can be determined through the metadata elements associated with the records, such as titles, dates, author, container number (where applicable), and other such attributes. Where these relationships exist between records imported or extracted from external business systems, the electronic records management system should be capable of identifying, capturing, documenting and preserving them.

These aggregations may be formal, structured relationships (for example, digital files containing related digital documents), or may exist as less formalised, tightly bound metadata relationships recognised as establishing links between related records within an aggregation.

The aggregations must be fixed and maintained over time. Any change to an

aggregation must be logged with an explanation. Aggregation for the management of records purposes should not be confused with, or replaced by, the generation of multiple, different aggregations in response to search requests or report queries.

Figure 2: Aggregation of records
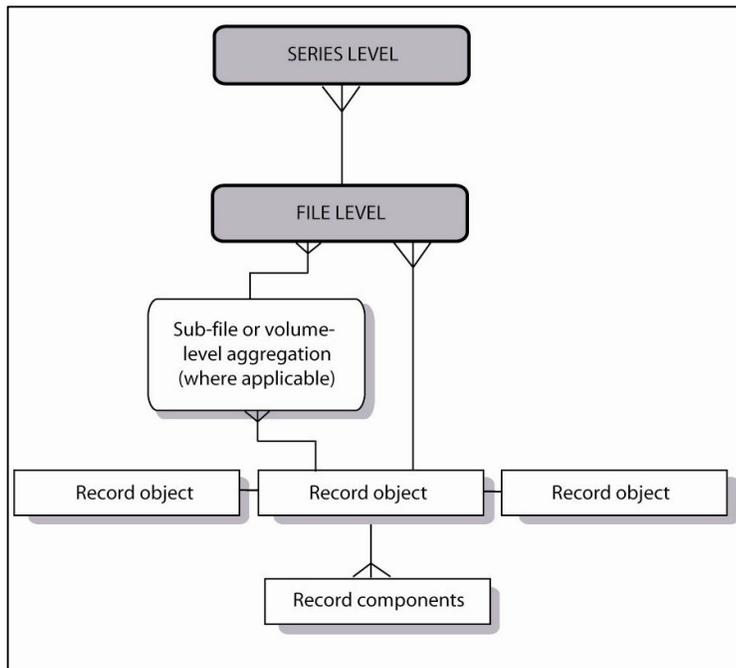
Identification (registration)

To verify their existence within the system, every record and associated aggregation must have a unique identifier persistently linked to it. This allows the user to locate records and helps them to distinguish between versions.

Classification

Within electronic records management systems implementations, aggregations are often used to enable inheritance of characteristics to records created or related at a lower level of aggregation. Typically in electronic records management systems, information is managed as record objects, and aggregates these objects into a set of series or files. Agencies should take into account their own business needs when determining suitable records aggregations (for example, by function, activity or transaction) within their agency. Within a business classification scheme, a record's contextual characteristics are attributed through structuring them according to identifiable business processes.

Functional classification schemes are based on an analysis of the unique business functions and activities of an organisation, and are independent of the organisation's administrative structure. This makes functional classification more flexible and stable as business units and structures are likely to change over time. This system breaks down traditional organisational information silos and enables easier retention and disposal.

Business classification scheme

A business classification scheme is a conceptual hierarchical classification tool that can facilitate the capture, titling, retrieval, maintenance and disposition of records. It defines the way in which records are grouped together (aggregated) and linked to the business context in which they were created or transmitted. For example, records in an organisation-wide electronic records management system in the public sector may be aggregated broadly into housekeeping and functional categories. The records in this two categories can be further aggregated into Business Functions, Main Activities and Sub Activities with their constituent record parts and contextual metadata, or may be subsequently aggregated into files. Records are often aggregated at five levels of granularity according to a five-tiered functional classification scheme as advocated by the National Archives of Malaysia as follows:

Figure 3: Five-tiered functional classification scheme

Level 1	Business Function
Aggregations of business functions referred to as 'class'	
Level 2	Main Activity
Series consisting of aggregations of main activities carried out under a particular business function. Can be a hierarchical level or may contain files/ 'containers'.	
Level 3	Sub Activity
Consists of aggregations of sub activities. May consists of files with individual records (referred to as 'containers'). Files may also be sub divided into volumes.	
Level 4	Sub-sub Activity
Aggregations of files with individual records. May be sub divided into volumes.	
Level 5	Transaction
Items – in this document referred to as 'records'. May be comprised of multiple components.	

Note: This is a basic model. Aggregations of more than five levels may be necessary depending on the business processes described, or for clearer definition of complex topics. However aggregations should be limited to a maximum of six levels.

The record (object) is located at the very bottom of the aggregation hierarchy. Some metadata values may be inherited from a higher layer of aggregation by all those files or objects located below. Regardless of how many levels of aggregation below series or file level are implemented, each level should be consistent with the metadata requirements for the higher aggregation level.

2.3.2 Maintain

Managing authentic and reliable records

Records captured into electronic records management systems must be actively maintained to ensure their continued accessibility. Establishing appropriate security controls, building in disposal outcomes and enabling the management of hybrid records facilitate comprehensive, authentic, useable, tamper-proof and appropriately disposed records.

Controls and security

Records captured into an electronic records management system must be protected against intentional or accidental alteration of their content, structure and context throughout their life to retain their authenticity. Electronic records management systems must control access to, or alteration of, metadata. Location tracking, access controls and control over any alteration of records ensure the authenticity of records in an electronic records management system.

Hybrid records management

Agencies typically manage records that span a range of electronic and non-electronic media. Electronic records management systems must be able to ingest and maintain records management metadata relating to non-electronic records as well as electronic records and any associated records management metadata. Essentially, contextually related records regardless of whether they are in electronic or non-electronic format must be managed and subject to the same records management processes within their aggregations.

To facilitate hybrid records management functionality, the electronic records management system must be able to capture and maintain metadata relating to physical records. This requires the creation of markers that are metadata profiles of records physically held outside the business system. Markers contain metadata required by the business system to locate and manage physical records and allocate system management controls to them. A marker may denote a physical record, such as a plan or paper file, or an electronic record or aggregation of electronic records stored on removable media, such as a CD-ROM or magnetic tape.

Retention and disposal

Record disposal schedule are policies that authorise the disposal of records, whether by destruction, transfer of control or applying a review period. Record disposal schedule consist of disposal actions and retention periods for

aggregations of records that may have a legislative or organisational use/requirement source. Organisations should review disposal actions when the relevant retention periods have expired.

Records are often transferred between electronic records management systems for a range of reasons other than disposal, for example, migration to a new electronic records management system as a result of a technology refresh or an organisational restructure. In all cases, where there is transfer of records (whether this involves movement to another electronic records management system or not) and/or subsequent destruction of records from the original electronic records management system, any existing records management metadata and point of capture metadata must be considered at the same time as the records to which they relate.

2.3.3 Use, Access and Dissemination

An electronic records management system must be able to search for, retrieve and render the records that it maintains. These functions facilitate useable records. Searching is the process of identifying records or aggregations through user-defined parameters so that the records, aggregations and/or their associated records management metadata can be retrieved. Search and navigation tools are required to locate records, aggregations or records management metadata by employing a range of searching techniques to cater for novice and sophisticated users. Retrieving is the process of preparing the located records for rendering and viewing.

Rendering is the production of a human-readable representation of a record, usually to a visual display screen or in hardcopy format. Electronic records management systems typically contain records in a range of file formats. The user must be able to have human-readable access to records stored in all these formats through an appropriate rendering interface. Where it is meaningful to print a hardcopy of a record, the electronic records management system must provide functionality to allow all users to obtain printed copies of records and their records management metadata where appropriate.

2.3.4 Administer (Records Maintenance Management)

As with most software applications, there is a need for a system administrator to undertake system maintenance and other support functions, such as maintenance of access groups and updating of the business classification system. Administration facilitates useable records, reliable systems, systematic practices and the routine application of records management procedures. This Module only refers to management of records administration that must be controlled and auditable to ensure the integrity, authenticity and reliability of the records.

2.4   Using the functional requirements set

This specification lists the set of functional requirements for the management of records in electronic systems. They are grouped according to the clusters from

the high-level model in Figure 1.

2.4.1 Key outcomes

The functional requirements focus on the outcomes required to ensure records are managed appropriately, regardless of the type of electronic records management system employed. As the functional requirements provide a high-level description of records management functionality rather than detailed specifications, it is recognised that the techniques and strategies to achieve the outcomes will depend on the type of system being used. It is intended that each organisation should tailor the functional requirements to meet its individual business needs.

2.4.2 Obligation levels

The keywords **'must'**, **'should'** and **'may'** that appear in the requirements in this specification indicate the relative importance of each requirement. These keywords are to be interpreted as follows:
* **Must** – requirements that use 'must' are necessary and is mandatory for compliance with the specification.
* **Should** – highly desirable to support the mandatory requirements.
* **May** – requirements that use 'may' are truly optional and may be incorporated or omitted as appropriate. This document reflects international consensus; the requirements and obligation levels are not jurisdictionally specific or legally binding. Users should asses their own legislative environmental issues, business requirements and risk assessments where appropriate.

3   FUNCTIONAL REQUIREMENTS

This part presents the set of functional requirements for electronic systems. They are divided into four sections according to key records management concepts and processes as outlined:

- Create
- Maintain
- Disseminate
- Administer
- Multimedia Repository
- Enterprise Content Management
- Collaboration Management

The functional requirements are focused on the outcomes required to ensure records are managed appropriately. They do not specify particular processes, as it is recognised that the techniques and strategies to achieve the outcomes will depend on the organisation and electronic records management system being used. The introductory text to each section provides summary information regarding the records management concept and the overarching aim of the subsequent requirements.

While they do not cover common system management and design requirements, such as interoperability, scalability and performance, it is acknowledged that such processes also support the recordkeeping functionality of the system. The functional requirements assume that a basic records management framework is in place, such as policies, procedures, and business retention and classification.

CREATE

3.1   Capture

Records are created in a diverse range of formats, may comprise multiple individual objects (compound records), and are transmitted by a wide range of communication channels (workflows, email, postal mail). Electronic records management systems must capture the content, structure and context of records to ensure they are reliable and authentic representations of the business activities or transactions in which they were created or transmitted. This is known as 'point of capture' metadata and should in itself be captured as a record; it should not be possible to alter any of these metadata features without changes being tracked and auditable.

3.1.1   Capture Processes

The electronic records management system **must**:

RM1	Enable integration with business applications so that transactional records created by those applications can be captured within the electronic records management system (including email, see Requirements 21–25).
RM2	Indicate when an individual record is captured within the electronic records management system.
RM3	Prevent the alteration of the content of any record by any user or administrator during the process of records capture. See also Requirements 88 and 89.
RM4	Prevent the destruction or deletion of any record by any user, including an

	administrator, with the exceptions of: • destruction in accordance with a disposition authority (see Section 3.6: Retention and disposal); and • authorised deletion by an administrator (see Section 3.8: Administration).
RM5	Support manual naming of electronic records, and allow this name to be different from the existing file name (including email subject lines used to construct record titles). If the existing filename is taken by default, the electronic records management system must allow this name to be amended at the time of capture.
RM6	Allow an administrator to alter the metadata of a record within the system if required, to allow finalisation/correction of the record profile. Any such action must be captured in a records management metadata.
RM7	Any revision or alteration of the records management/capture metadata must be captured as additional records management metadata.
RM8	Alert a user to any failure to successfully capture a record.
RM9	Be able, where possible and appropriate, to provide a warning if an attempt is made to capture a record that is incomplete or inconsistent in a way which will compromise its future apparent authenticity.
RM10	Capture scanned images of incoming documents.

3.1.2 Point Of Capture Metadata

To be meaningful as evidence of a business process, records must be linked to the context of their creation and use. In order to do this, the record must be associated with metadata about the business context in which it was created and its point of capture into the system.

Much of this information can be automatically generated by the system. It is expected that each organisation will capture records management metadata in line with an identified records management metadata standard (compliant with ISO 23081), and organisational and/or jurisdictional requirements.

The electronic records management system **must**:

RM11	Support the use of persistent metadata for records
RM12	Acquire metadata elements for each record and persistently link them to the record over time.
RM13	Ensure that the values for metadata elements conform to specified encoding schemes.
RM14	Allow the administrator to pre-define (and re-define) the metadata elements associated with each record, including whether each element is mandatory or optional.
RM15	Allow all metadata for every record to be viewed by users, subject to access rights for individuals or groups of users.
RM16	Automatically capture the date and time of capture of each record as metadata elements linked to each record.
RM17	Support automatic extraction or migration of metadata from: • the software application that created the record; • an operating system or line of business system; • an electronic records management system; and

	• the file header, including file format metadata, of each record and its constituent components captured into the system.
RM18	Prevent the alteration of metadata captured in Requirement 16, unless authorised by the system administrator.
RM19	Allow entry of additional metadata by users during record capture and/or a later stage of processing by the user.
RM20	Ensure that only authorised users and administrators can change the content of records management metadata elements.
RM21	Allocate an identifier, unique within the system, to each record at point of capture automatically.

3.1.3 Aggregation Of Electronic Records

Aggregations of electronic records are accumulations of related electronic record entities that when combined may exist at a level above that of a singular electronic record object, for example, a file or series. These relationships are reflected in the metadata links and associations that exist between the related electronic records, and between the electronic records and the system. For example, an aggregation of electronic records may collectively constitute a narrative of events (that is, a series of connected business transactions), in which the records may have a sequential relationship. Any such sequential relationship between electronic records can be determined through the metadata elements associated with the records, such as titles, dates, author, container number (where applicable), and other attributes. Where these relationships exist between records controlled by the electronic records management system, the system should be capable of identifying, capturing, documenting and maintaining or systematically disposing of them.

The electronic records management system **must**:

RM22	Ensure that all records captured within the electronic records management system are associated with at least one aggregation.
RM23	Manage the integrity of all markers or other reference tags to records (where used), ensuring that: • following a marker, whichever aggregation that the marker record is located in, will always result in correct retrieval of the record; and • any change in location of a record also redirects any marker that references that record.
RM24	Not impose any practical limit on the number of records that can be captured in an aggregation, or on the number of records that can be stored in the electronic records management system. However, the system may permit the administrator to set limitations on the quantity of items within an aggregation if required for business purposes.
RM25	Allow users to choose at least one of the following where an electronic object has more than one manifestation: • register all manifestations of the object as one record; • register one manifestation of the object as a record; or • register each manifestation of the object as a discrete record.

The electronic records management system **should**:

RM26	Support the ability to assign records to multiple aggregations without their duplication. [5]

3.1.4 Bulk Importing

Records and their metadata may be captured into an electronic records management system in bulk in a number of ways, for example, from another electronic records management system or as a bulk transfer from an electronic document management system or workflow application. The electronic records management system must be able to accept these, and must include features to manage the bulk capture process.

The electronic records management system **must**:

RM27	Be able to capture in bulk records exported from other systems, including capture of: • electronic records in their existing format, without degradation of content or structure, retaining any contextual relationships between the components of any individual record; • electronic records and all associated records management metadata, retaining the correct contextual relationships between individual records and their metadata attributes; and • the structure of aggregations to which the records are assigned, and all associated records management metadata, retaining the correct relationship between records and aggregations. [6]
RM28	Be able to import any directly associated event history metadata with the record and/or aggregation, retaining this securely within the imported structure.

3.1.5 Electronic Document Formats

Electronic records management systems will have to deal with a range of formats, both common applications and often business-specific formats. The electronic records management system must have the functionality to deal with the formats that you commonly use or are common to your business environment. This will vary across systems and organisations.

For ease of migration and export, use of open formats and industry standards will increase levels of interoperability and reduce the cost and difficulty of maintaining records effectively.

---

[5] For example, an invoice might be added to a supplier file by one user and to a product file by another. This could be achieved by using a marker system.

[6] For example, maintaining a persistent embedded metadata record of the original classification

The electronic records management system **must**:

RM29	Support the capture of records created in native file formats from commonly used software applications such as: • standard office applications (word processing, spread-sheeting, presentation, simple databases); • email client applications; • imaging applications; and • web authoring tools. Not apply any practical limit to record types or format for capture.
RM30	Be able to extend the range of file formats supported as new file formats are introduced for business purposes or for archival retention (for example, PDF/A).[7]

3.1.6 Compound Records

Electronic records will comprise at least one component. An electronic record such as a text document will usually be a discrete record and comprise a single record object. Electronic records that comprise more than one component or multiple record objects, for example, a large technical report with dynamic links to diagrams and spreadsheets, may be referred to as 'compound records'.

The nature of the components that comprise a given electronic record will vary. A component may be an electronic object, such as an electronic document, or a data element, such as an entry in a database. For example, a component of an electronic record in a system that encompasses the management of documents may consist of a single word-processed document, while components forming an electronic record in a human resource management system may comprise a number of closely linked data entries in a database (such as all data entered in connection with a single staff member's personnel profile). These compound records should not be confused with internal record components or elements, such as a record object and its metadata or physical document and its marker.

The electronic records management system **must**:

RM31	Capture compound electronic records (records comprising more than one component) so that: • the relationship between the constituent components of each compound record is retained; • the structural integrity of each compound record is retained; and • each compound record is retrieved, displayed and managed as a single unit.
RM32	Be able to capture compound records easily, preferably with one action, for example, a single click.

---

[7] It is not always possible to capture specialised records (or those from specialised systems) with an electronic records management system; however, this risk should be mitigated against. Strategies for normalisation of formats for capture or a process of capturing the entire system should be considered. Where this is not possible, building records management capability into the business information system should be considered.

3.1.7 Email

Email is used for sending both simple messages and documents (as attachments), within and between organisations. The characteristics of email can make it difficult to track and register. Organisations must provide users with the capability of capturing selected email messages and attachments.

The electronic records management system **must**:

RM33	Allow users to capture emails (text and attachments) as single records as well as individual records linked by metadata
RM34	Allow individual users to capture email messages (and attachments) from within their email application.
RM35	Allow users to choose whether to capture emails with attachments as: • email text only; • email text with attachments; or • attachments only.[8]
RM36	Ensure the capture of email transmission data as metadata persistently linked to the email record.
RM37	Ensure that the text of an email and its transmission details cannot be amended in any way once the email has been captured. Nor should the subject line of the email itself be changeable, although the title of the record may be edited for easier access through, for example, keywords or by file-naming conventions.
RM38	Ensure that a human-readable version of an email message address is also captured, where one exists.[9]

3.2 Identification

To verify their existence within a system, every record and associated aggregation must have a unique identifier persistently linked to it. This allows to the user to locate records and helps them to distinguish between versions.

The electronic records management system **must**:

RM39	Associate each of the following with a unique identifier: • record; • record extract; and • aggregation
RM40	Require all identifiers to be unique and unduplicated within the entire electronic records management system.
RM41	Be able to store the unique identifiers as metadata elements of the entities to which they refer
RM42	Generate unique identifiers automatically, and prevent users from inputting the unique identifier manually and from subsequently modifying it (for example, a

---

[8] It is essential that these processes are recorded and embedded within the metadata of the records. The user must be alerted to the existence of the related items.

[9] For example, for 'Samuel Johnson' <samjo@worldintnet.org> – 'Samuel Johnson' is the human- readable version of the email address samjo@worldintnet.org.

	sequential number)
RM43	Allow the format of the unique identifier to be specified at configuration time.[10]

Where unique identifiers are automatically generated, the electronic records management system **should**:

RM44	Allow the administrator to specify at configuration time the starting number (for example, 1, 10, 100) and increment (for example, 1, 10) to be used in all cases.

3.3   Classification

3.3.1 Establishing A Classification Scheme

A records classification scheme is a hierarchical classification tool that can facilitate the capture, titling, retrieval, maintenance and disposal of records. A classification scheme lies at the heart of any electronic records management system since it defines the way in which individual electronic records are grouped together (aggregated) and linked to the business context in which they were created or transmitted. By aggregating records, many of the records management processes described below can be carried out quickly and efficiently.

The electronic records management system **must**:

RM45	Support and be compatible with the organisational classification scheme.
RM46	Be able to support a classification scheme that can represent aggregations (at the function, activity, transaction level) as being organised in a hierarchy with a **minimum** of five levels.
RM47	Allow the inheritance of values from a classification scheme.
RM48	Allow naming conventions or thesauri to be defined at the time the electronic records management system is configured.
RM49	Support the initial and ongoing construction of a classification scheme.
RM50	Allow administrators to create new aggregations at any level within any existing aggregation.
RM51	Not limit the number of levels in the classification scheme hierarchy unless set by an administrator.
RM52	Support the definition of different record types that are associated with a specified set of metadata to be applied at capture.
RM53	Support the allocation of unique identifiers to records within the classification structure

Where the unique identifiers are based on sequential numbering, the electronic records management system **should**:

RM54	Have the capacity to automatically generate the next sequential number within the classification scheme for each new electronic aggregation.11[11]

---

[10] The identifier may be numeric or alphanumeric, or may include the concatenated identifiers of the volume and electronic aggregations above the record in the classification scheme.

[11] For example, if the following aggregations are within a classification scheme:
• 900 - 23 - 01 Manufacturing : Order Processing : Sales Order Validation;

The electronic records management system **may**:

RM55	Support a distributed classification scheme that can be maintained across a network of electronic record repositories.

Where the electronic records management system employs a graphical user interface, it **must**:

RM56	Support browsing and graphical navigation of the aggregations and classification scheme structure, and the selection, retrieval and display of electronic aggregations and their contents through this mechanism.

The electronic records management system **should**:

RM57	Support the definition and simultaneous use of multiple classification schemes. This may be required, for example, following the merger of two organisations or migration of legacy systems. It is not intended for routine use.

3.3.2 Classification Levels

The electronic records management system **must**:

RM58	Support metadata for levels within the classification scheme.
RM59	Provide at least two naming mechanisms for records in the classification scheme: • a mechanism for allocating a structured alpha, numeric or alphanumeric reference code (that is, an identifier which is unique within the classification scheme) to each classification level; and • a mechanism to allocate a textual title for each electronic aggregation. It must be possible to apply both identifiers separately or together.
RM60	Allow only authorised users to create new classifications at the highest level in the classification scheme (for example, at the business function level).
RM61	Record the date of opening of a new aggregation within its associated records management metadata.
RM62	Automatically include in the records management metadata of each new aggregation those attributes that derive from its position in the classification scheme (for example, name, classification code).[12]
RM63	Allow the automatic creation and maintenance of a list of classification levels

The electronic records management system **should**:

RM64	Support a naming mechanism that is based on controlled vocabulary terms and relationships drawn (where appropriate) from an ISO 2788-compliant or ISO

• 900 - 23 - 02 Manufacturing : Order Processing : Invoicing;
• 900 - 23 - 03 Manufacturing : Order Processing : Credit Note Processing;
and the administrator adds a new aggregation to the 'Order Processing' aggregation, the electronic records management system should automatically assign it the reference 900 - 23 - 04. Likewise, if the administrator adds a new class to the 'Manufacturing' aggregation, the electronic records management system should automatically assign it the reference 900 - 24.

[12] For example, if a file is in a hierarchical path: 'Regional plan development : Public consultation :Public submissions'and the administrator adds a new file named 'Formal objections' at the same level as the 'Public submissions' file, then it must automatically inherit the prefix 'Regional plan development : Public consultation'.

	5964-compliant thesaurus and support the linking of the thesaurus to the classification scheme
RM65	Support an optional aggregation naming mechanism that includes names (for example, people's names) and/or dates (for example, dates of birth) as file names, including validation of the names against a list
RM66	Support the allocation of controlled vocabulary terms compliant with ISO 2788 or ISO 5964 as records management metadata, in addition to the other requirements in this section

3.3.3 Classification Processes

The electronic records management system **must**:

RM67	Allow an electronic aggregation (including volumes) to be relocated to a different position in the classification scheme, and ensure that all electronic records already allocated remain allocated to the aggregations (including volumes) being relocated.[13]
RM68	Allow an electronic record to be reclassified to a different volume of an electronic aggregation.[14]
RM69	Restrict to Administrators and Records Manager the ability to move aggregations (including volumes) and individual records.
RM70	Keep a clear history of the location of reclassified aggregations (including volumes) prior to their reclassification, so that their entire history can be determined easily.[15]
RM71	Prevent the deletion of an electronic aggregation or any part of its contents at all times, with the exceptions of: • destruction in accordance with a disposal authority; and • deletion by an administrator as part of an audited procedure.
RM72	Allow an electronic aggregation to be closed by a specific administrator procedure, and restrict this function to an administrator.
RM73	Record the date of closing of a volume in the volume's records management metadata.
RM74	Maintain internal integrity (relational integrity or otherwise) at all times, regardless of: • maintenance activities; • other user actions; and • failure of system components.[16]

---

[13] This facility is intended for exceptional circumstances only, such as organisational mergers or other re-organisation, or to correct clerical errors. This requirement must be read together with Requirements 71, 72 and 81.

[14] This facility is intended for exceptional circumstances only, such as to correct clerical errors. This requirement must be read together with Requirements 71, 72 and 81.

[15] At a minimum, this must be stored in the metadata. It may also be desirable to record it elsewhere, for example, in the records management metadata of the object(s) being moved.

[16] That is, it must be impossible for a situation to arise where any user action or any software failure results in an inconsistency within the electronic records management system or its database.

RM75	Not allow any volume that has been temporarily re-opened to remain open after the administrator who opened it has logged off.
RM76	Allow users to create cross-references between related aggregations or between aggregations and individual records.
RM77	Provide reporting tools for the provision of statistics to the administrator on aspects of activity using the classification scheme, including the numbers of electronic aggregations (including volumes) or records created, closed or deleted within a given period, by user group or functional role.
RM78	Allow the Administrators and Records Manager to enter the reason for the reclassification of aggregations (including volumes) and individual records.
RM79	Be able to close a volume of an electronic aggregation automatically on fulfillment of specified criteria to be defined at configuration, including at least: • volumes delineated by an annual cut-off date (for example, end of the calendar year, financial year or other defined annual cycle); • the passage of time since a specified event (for example, the most recent addition of an electronic record to that volume); and • the number of electronic records within a volume.[17]
RM80	Be able to open a new volume of an electronic aggregation automatically on fulfillment of specified criteria to be defined at configuration
RM81	Allow an administrator to lock or freeze aggregations to prevent relocation, deletion, closure or modification when circumstances require, for example, pending legal action

3.3.4 Record Volumes

This section includes requirements relating to the use of volumes, which are typically used to subdivide aggregations that might otherwise be unmanageably large. The requirements for volumes only apply to the aggregations at the activity level.

Where the electronic records management system uses volumes, it **must**:

RM82	Allow administrators to add (open) electronic volumes to any electronic aggregation that is not closed.
RM83	Record the date of opening of a new volume in the volume's records management metadata.
RM84	Automatically include in the metadata of new volumes those attributes of its parent aggregation's records management metadata that assign context (for example, name, classification code).
RM85	Support the concept of open and closed volumes for electronic aggregations, as follows: • only the most recently created volume within an aggregation can be open; and • all other volumes within that aggregation must be closed (subject to temporary exceptions required by Requirement 68).[18]
RM86	Prevent the user from adding electronic records to a closed volume (subject to the exceptions required by Requirement 69).

---

[17] Other criteria may be desirable in particular circumstances, for example, where the size of the volume reaches the capacity of storage media.

[18] Note that the records in a volume can be accessed regardless of whether the volume is open or closed.

MAINTAIN

3.4 Managing Authentic And Reliable Records

3.4.1 Access And Security

Organisations need to control access to their records. Typically, access to records and aggregations is limited to specific users and/or user groups. In addition to controlling access by user and user groups, some agencies will need to limit access further by using security classifications. This is achieved by allocating security classifications to aggregations and/or records. Users can then be allocated security clearances to permit selective access to aggregations or records at higher security categories.

Maintaining metadata of all records management actions undertaken by an electronic records management system and its users and administrators is essential to meeting requirements for legal admissibility. This process is also known as 'tracking'.

Over time, records and aggregations may be transferred from one storage medium or location to another (for example, migration), as their activity decreases and/or their use changes. A tracking feature is needed to record the change of location for both ease of access and to meet regulatory requirements.

The electronic records management system **must**:

RM87	Ensure that records are maintained complete and unaltered
RM88	Maintain the technical, structural and relational integrity of records and metadata in the system.

3.4.2 Access Controls

The electronic records management system **must**:

RM89	Restrict access to system functions according to a user's role and strict system administration controls.[19]

3.4.3 Establishing Security Control

Normal systems controls over access and security support the maintenance of authenticity, reliability, integrity and usability, and therefore should be appropriately implemented.

For example, in a high-risk environment, it may be necessary to prove exactly what happened, when and by whom. This links to systems permissions and audit logging, to prove that approved actions are undertaken by authorised people.

The electronic records management system **must**:

RM90	Allow only administrators to set up user profiles and allocate users to groups.

---

[19] For example, an unauthorised user access attempt.

RM91	Allow the administrator and Records Manager to limit access to records, aggregations and records management metadata to specified users or user groups.
RM92	Allow the administrator and Records Manager to alter the security category of individual records.[20]
RM93	Allow changes to security attributes for groups or users (such as access rights, security level, privileges, initial password allocation and management) to be made only by the administrator.

3.4.4 Assigning Security Levels

The electronic records management system **must**:

RM94	Allow only the administrator and Records Manager to attach to the user profile attributes that determine the features, records management metadata fields, records or aggregations to which the user has access. The attributes of the profile will: • prohibit access to the electronic records management system without an accepted authentication mechanism attributed to the user profile; • restrict user access to specific records or aggregations; • restrict user access according to the user's security clearance; • restrict user access to particular features (for example, read, update and/or delete specific records management metadata fields); • deny access after a specified date; and • allocate the user to a group or groups.[21]
RM95	Be able to provide the same control functions for roles, as for users.[22]
RM96	Be able to set up groups of users that are associated with an aggregation.[23]
RM97	Allow a user to be a member of more than one group.

If the electronic records management system maintains a list of aggregations, it **must**:

RM98	Be able to limit users' access to parts of the list (to be specified at the time of configuration).

3.4.5 Executing Security Controls

The electronic records management system **must**:

RM99	Allow the administrator and Records Manager, subject to Section 3.4.6: Security Categories, to alter the security category of all records within an aggregation in one operation. The electronic records management system

---

[20] This is routinely required to reduce the level of protection given to records as their sensitivity decreases over time.

[21] An example of an accepted authentication mechanism is a password.

[22] This feature allows the administrator to manage and maintain a limited set of role access rights rather than a larger number of individual users. Examples of roles might include Manager, Claims, Processing Officer, Security Analyst or Database Administrator.

[23] Examples of groups might be Personnel or Sales Team.

	must provide a warning if the security classifications of any records are lowered, and await confirmation before completing the operation.[24]
RM100	Allow the administrator and Records Manager to change the security category of aggregations, subject to the requirements of Section 3.4.6: Security Categories.
RM101	Record full details of any change to security category in the records management metadata of the record, volume or aggregation affected.
RM102	Provide one of the following responses (selectable at configuration time) whenever a user requests access to, or searches for, a record, volume or aggregation that they do not have the right to access: • not display any record information or indicate its existence in any way.[25]
RM103	Never include, in a list of full text or other search results, any record that the user does not have the right to access.
RM104	Log all unauthorised attempts to access aggregations (and their volumes) or records in their respective unique metadata.[26]

3.4.6 Security Categories

The functional requirements in this section only apply to organisations that manage classified records within their electronic records management system. Please refer to your jurisdictional requirements and security requirements.

The electronic records management system **must**:

RM105	Allow security classifications to be assigned to records.[27]
RM106	Allow security classifications to be selected and assigned at system level for: • all levels of records aggregations (including volumes); and • individual records or record objects.
RM107	Allow access-permission security categorisation to be assigned: • at group level (be able to set up group access to specific aggregations, record classes security or clearance levels); • by organisational role; • at user level; and

---

[24] This is routinely required to reduce the level of protection given to records as their sensitivity decreases over time.

[25] This option is the most stringent and it implies that the electronic records management system must not include such records in any count of search results. This is also in keeping with the requirements of The Security Instruction issued by The Chief Government Security Officer.

[26] It will be acceptable for this feature to be controllable so that it only applies to administrator-specified security categories. Although the system should capture the location/interface and user or user log-in that attempted to gain access.

[27] Security classification will be jurisdictionally or organisationally assigned in Malaysia as specified in The Security Instruction issued by The Chief Government Security Officer is as follows:

- Top Secret
- Secret
- Confidential
- Restricted

Further caveats may be assigned to any security clearance levels.

	• in combination(s) of the above.[28]
RM108	Allow the assignment of a security category: • at any level of records aggregation; • after a specified time or event; and • to a record type.[29]
RM109	Support the automated application of a default value of 'Unclassified' to an aggregation or record not allocated any other security category.
RM110	Enable its security subsystem to work effectively together with general security products.
RM111	Be able to determine the highest security category of any record in any aggregation by means of one simple enquiry.
RM112	Support routine, scheduled reviews of security classifications.
RM113	Restrict access to electronic aggregations/records that have a security classification higher than a user's security clearance.

If security classifications are assigned to aggregations as well as individual records (as per Requirement 105, then the electronic records management system **must**:

RM114	Be capable of preventing an electronic aggregation from having a lower security classification than any electronic record within that aggregation.

3.4.7 Records Management Process Metadata

Metadata about the processes of managing the record, including the disposal of the record, needs to be documented to ensure the integrity and authenticity of the record, so that all alterations, linkages and uses of the record are able to be authoritatively tracked over time. Records exist at different layers of aggregation, for example, as documents/items, files or series. Records management metadata must be applied to records at all levels of aggregations. Although the record may be fixed and inviolable, the records management metadata will continue to accrue throughout the administrative life of the record. It must be persistently linked to the record to ensure that the record is authentic, unaltered and reliable.

The electronic records management system **must**:

RM115	Be capable of creating unalterable metadata of records management actions (actions to be specified by each agency) that are taken on records, aggregations or the classification scheme. The metadata should include the following records management metadata elements: • type of records management action; • user initiating and/or carrying out the action; and • date and time of the action.[30]

---

[28] This will allow an administrator to manage and maintain a limited set of access-permissions/categories based on roles within the organisation rather than managing a large number of individual user-permission profiles for classified access.

[29] Note that the correct level of security clearance may not be sufficient to obtain access. Searches will block access by not returning search results for records that are above a searcher's access clearance, see Requirements 102.

RM116	Track events without manual intervention and store information in the metadata once the metadata functionality has been activated.
RM117	Maintain the metadata for as long as required.
RM118	Provide metadata of all changes made to: • electronic aggregations (including volumes); • individual electronic records; and • records management metadata associated with any of the above.
RM119	Document all changes made to administrative parameters (for example, changes made by the administrator to a user's access rights).
RM120	Be capable of capturing and storing in the metadata information about the following actions: • date and time of capture of all electronic records; • reclassification of an electronic record in another electronic volume; • reclassification of an electronic aggregation in the classification scheme; • any change to the disposal authority of an electronic aggregation; • any change made to any records management metadata associated with aggregations or electronic records; • date and time of creation, amendment and deletion of records management metadata; • changes made to the access privileges affecting an electronic aggregation, electronic record or user; • export or transfer actions carried out on an electronic aggregation; • date and time at which a record is rendered; and • disposal actions on an electronic aggregation or record.
RM121	Be able to export metadata for specified records and selected groups of records without affecting the metadata stored by the electronic records management system.[31]
RM122	Be able to capture and store violations (that is, a user's attempts to access a record or aggregation, including volumes, to which they are denied access), and (where violations can validly be attempted) attempted violations of access control mechanisms.[32]
RM123	Be able, at a minimum, to provide reports for actions on records and aggregations organised: • by record or aggregation; • by file listing (list of entire files in e-file plan/classification scheme) • by file listing and description • by user; and • in chronological sequence of all actions in system
RM124	Allow the metadata facility to be configurable by the administrator so that the functions for which information is automatically stored can be selected. The electronic records management system must ensure that this selection and all

[30] The word 'unalterable' means that the metadata data cannot be modified in any way or deleted by any user.

[31] This functionality can be used by external auditors who wish to examine or analyse system activity.

[32] It is acceptable for this feature to be controllable so that it only applies to administrator-specified security categories.

	changes to it are stored in the metadata.
RM125	Be able to provide reports for actions on aggregations and records organised by workstation and (where technically appropriate) by network address.
RM126	Allow the administrator to change any user-entered records management metadata element. Information about any such change must be stored in the metadata.[33]

3.4.8 Tracking Records Movement

Location can refer to the physical location for hybrid records or the location within a classification structure or file structure for electronic records. Movement refers to changing the location of both electronic and physical records.

The electronic records management system **must**:

RM127	Provide a tracking feature to monitor and record information about the location and movement of both electronic and non-electronic aggregations.
RM128	Record information about movements including: • unique identifier of the aggregation or record; • current location as well as a user-defined number of previous locations (locations should be user-defined); • date item sent/moved from location; • date item received at location (for transfers); and • user responsible for the move (where appropriate).
RM129	Maintain access to the electronic record content, including the ability to render it, and maintenance of its structure and formatting over time and through generations of office application software.[34]

3.5   Hybrid Records Management

3.5.1 Management of Electronic And Non-Electronic Records

These functional requirements include requirements for hybrid system management. It includes functionality for managing records and files in both physical and electronic format.

Hybrid file

The relationship between physical files and records in electronic formats differs significantly. As physical records (such as paper-based files) cannot be physically captured and registered directly into the business system, the business system must create and maintain markers – metadata profiles of physical records – to maintain linkages between the physical and electronic files.

Generally the marker will identify the title and unique identifier of the physical record,

---

[33] This functionality is intended to allow administrators to correct user errors, such as data input errors, and to maintain user and group access.

[34] This may be achieved by use of a multi-format viewer application.

outline the record's content and provide location information for retrieval.

A hybrid file exists where a related set of physical files and aggregations of electronic records (for example, electronic files) deals with the same function, activity or transaction, and must be managed as a single aggregation of records. Management of these hybrid files involves merging the aggregation of electronic records and physical file management processes.

Hybrid records

Electronic records can be linked to physical records or files through a tightly bound metadata relationship to form a hybrid record, in much the same way that physical files and aggregations of electronic records can be linked to create hybrid files. The metadata link between the electronic and physical records will be established through the marker, which will identify the physical record and its location. The marker may be attached directly to the electronic record component of the hybrid record.

The electronic records management system **must**:

RM130	Be able to define in the classification scheme non-electronic aggregations and volumes, and must allow the presence of non-electronic records in these volumes to be reflected and managed in the same way as electronic records.
RM131	Allow both kinds of records to be managed in an integrated manner.
RM132	Allow a non-electronic aggregation that is associated as a hybrid with an electronic aggregation to use the same title and numerical reference code, but with an added indication that it is a hybrid non-electronic aggregation.
RM133	Allow a different records management metadata element set to be configured for non-electronic and electronic aggregations; non-electronic aggregation records management metadata must include information on the physical location of the non-electronic aggregation.
RM134	Ensure that retrieval of non-electronic aggregations displays the records management metadata for both electronic and non-electronic records associated with it.
RM135	Include features to control and record access to non-electronic aggregations, including controls based on security category, which are comparable with the features for electronic aggregations.
RM136	Support tracking of non-electronic aggregations by the provision of request, check-out and check-in facilities that reflect the current location of the item concerned.

The electronic records management system **should**:

RM137	Support the printing and recognition of bar codes for non-electronic objects (for example, documents, files and other containers), or should support other tracking systems to automate the data entry for tracking the movement of such non-electronic records.
RM138	Support the retention and disposal protocols and routinely apply to both electronic and non-electronic elements within hybrid aggregations.

Where aggregations have security categories, the electronic records management system **must**:

RM139	Ensure that a non-electronic record is allocated the same security category as an associated electronic record within a hybrid records aggregation.

3.6   Retention And Disposal

3.6.1 Records Disposal Schedule

'Disposal' according to the National Archives Act 2003 means the manner of managing the segregation of records with a view to destruction, transfer or otherwise. In this specification the term 'disposition' is used to cover all these processes and the term 'disposal' is used as shorthand for assigning a period before authorised destruction can be considered.

Deletion is often considered to be (permanent) destruction; however material may still be accessible, discoverable or recoverable due to back-ups, personal hard drives and so on, and through digital forensics. Departments must ensure that all records that have to be deleted upon maturity of their retention periods as specified in the records disposal schedule are deleted in such a manner that it cannot be recovered or reconstructed in any manner what so ever. Methods for destruction are specified in Section 28.3, Chapter 4 of the IT Instruction 2007.

Establishing disposition authorities

The electronic records management system **must**:

RM140	Provide a function that: • specifies disposal authorities; • automates reporting and destruction actions; • disposes of compound records as a single action; and • provides integrated facilities for exporting records and records management metadata.
RM141	Be able to restrict the setting up and changing of records disposal schedule to the administrator and Records Manager.
RM142	Allow the administrator to define and store a set of customised standard records disposal schedule.

Applying records disposal schedule

The electronic records management system **must**:

RM143	Be capable of assigning a records disposal schedule to any aggregation or record type.
RM144	By default, ensure that every record in an aggregation is governed by the records disposal schedule associated with that aggregation.
RM145	Include a disposition action, agency retention period and trigger in the (metadata) record for the decision for each records disposal schedule.
RM146	For each aggregation: • automatically track retention periods that have been allocated to the aggregation; and • initiate the disposition process by prompting the administrator to consider

	and, where appropriate approve and execute, disposal action when disposition is due.
RM147	Allow at least the following decisions for each records disposal schedule: • retain indefinitely; • present for review after a specified date or timeframe; • destroy after a specified date or timeframe; and • transfer after a specified date or timeframe.
RM148	Allow retention periods for each records disposal schedule to be specified with the date which is able to be set in at least the following ways: • Date Created; • Date Closed; • Date Registered; • Last Action Date; • Date Modified; • Date Archived; • User Defined[35];
RM149	Enable a retention period to be assigned to an aggregation that over-rides the retention period assigned to its 'parent' aggregation.[36]
RM150	Allow the administrator to amend any retention period allocated to any aggregation at any point in the life of that aggregation.
RM151	Allow the administrator to change the retention period associated with an aggregation at any time.
RM152	Allow the definition of sets of processing rules that can be applied as an alerting facility to specified aggregations prior to initiation of a disposal process.[37]
RM153	Provide the option of allowing electronic records or aggregations that are being moved between aggregations by the administrator or records manager to have the retention period of the new aggregation, replacing the existing retention period applying to these records.

Executing records disposal schedules

The electronic records management system **must**:

RM154	Allow the administrator to delete aggregations, volumes and records upon maturity of their retention periods as specified in the records disposal

---

[35] The user defined date can be used by an organization for any purpose such as date of birth, for personal files etc. For example a disposal trigger or retention period can be expressed as "destroy 7 years after permanent archive" or "destroy 7 years after last action". The triggers should be able to calculate for the following actions :
- Make inactive
- Local archive
- Interim archive
- Permanent archive (transfer to National Archives of Malaysia)
- Destroy

[36] For example if an aggregation ('parent') contains another aggregation ('child'), then it must be possible to assign a retention period to the 'child' that over-rides the retention period for the 'parent'.

[37] For example, during a review of the aggregation and contents by a manager or administrator, notify the administrator when an aggregation has a given security level.

	schedules
RM155	When executing records disposal schedules, the electronic records management system must be able to: • produce an exception report for the administrator; • delete the entire contents of an aggregation or volume including backup copies when it is deleted to ensure the deletion is irreversible and the information cannot be recovered or reconstructed; • prompt the administrator to enter a reason for the action; • inform the administrator of any links from another aggregation or record to an aggregation or volume, that is about to be deleted, and request confirmation before completing the deletion; • alert the administrators to any conflicts, for example, items that are linked to more than one disposition action involving pointers; and • maintain complete integrity of the records management metadata at all times.

If more than one records disposal schedules are associated with an aggregation, the electronic records management system **must**:

RM156	Automatically track all retention periods specified in these records disposal schedules, and initiate the disposal process once the last of all these retention dates is reached.
RM157	Allow the administrator to manually or automatically lock or freeze records disposition processes (freeze for litigation or legal discovery purposes, Freedom of Information purposes, etc.).

Documenting disposition actions

The electronic records management system **must**:

RM158	Record any deletion or disposal action comprehensively in the process metadata.
RM159	Automatically record and report all disposal actions to the administrator.

Reviewing disposition

The electronic records management system **must**:

RM160	Support the review process by presenting electronic aggregations to be reviewed, with their records management metadata and information on retention periods, in a manner that allows the reviewer to browse the contents of the aggregation and/or records management metadata efficiently.
RM161	Allow the reviewer to take at least any one of the following actions for each aggregation during review: • mark the aggregation for destruction; • mark the aggregation for transfer; • mark the aggregation for indefinite hold, for example, pending litigation; and • change the disposal authority (or assign a different schedule) so that the aggregation is retained and re-reviewed at a later date, as defined in this section.
RM162	Allow the reviewer to enter comments into the aggregation's records management metadata to record the reasons for the review decisions.
RM163	Alert the administrator to aggregations due for disposal before implementing

	disposal actions, and seek confirmation from the administrator before initiating the disposal actions.
RM164	Always seek confirmation of disposal actions twice before proceeding.
RM165	Store in the metadata all decisions taken by the reviewer during reviews.
RM166	Produce a records disposal schedules report for the administrator that identifies all retention periods that are due to be applied in a specified time period, and provide quantitative reports on the quantity and types of records covered.
RM167	Be able to specify the frequency of a records disposal schedules report, the information reported and highlight exceptions such as overdue disposal.
RM168	Alert the administrator if an electronic aggregation that is due for destruction is referred to in a link from another aggregation and pause the destruction process to allow the following remedial action to be taken: • confirmation by the administrator to proceed with or cancel the process; and • generation of a report detailing the aggregation or record(s) concerned and all references or links for which it is a destination.
RM169	Support reporting and analysis tools for the management of records disposal schedules by the administrator, including the ability to: • list all retention periods; • list all electronic aggregations to which a specified records disposal schedule/retention period is assigned; • list the retention periods applied to all aggregations below a specified point in the hierarchy of the classification scheme; • identify, compare and review retention periods (including their contents) across the classification scheme; and • identify formal contradictions in retention periods across the classification scheme.
RM170	Provide, or support the ability to interface with, a workflow facility to support the scheduling, review and export/transfer process by tracking: • progress/status of the review, such as awaiting or in-progress, details of reviewer and date; • records awaiting disposal as a result of a review decision; and • progress of the transfer process.

The electronic records management system **should**:

RM171	Be able to accumulate statistics of review decisions in a given period and provide tabular and graphic reports on the activity.

3.6.2 Migration And Export

The electronic records management system **must**:

RM172	Provide a well-managed process to transfer records to another system or to a third party organisation and support migration processes.
RM173	Include all aggregations, volumes, records and associated metadata within aggregations whenever an electronic records management system transfers any aggregation or volume.
RM174	Be able to transfer or export an aggregation (at any level) in one sequence of operations so that: • the content and structure of its electronic records are not degraded; • all components of an electronic record (when the record consists of more

	than one component) are exported as an integral unit including any technical protection measures; • all links between the record and its records management metadata are retained; and • all links between electronic records, volumes and aggregations are retained.
RM175	Be able to include a copy of the entire metadata set associated with the records and aggregations that are transferred or exported from an electronic records management system.
RM176	Provide a utility or conversion tool to convert the entire metadata set associated with the records and aggregations that are transferred or exported into XML format[38].
RM177	Produce a report detailing any failure during a transfer, export or destruction. The report must identify any records destined for transfer that have generated processing error, and any aggregations or records that are not successfully transferred, exported or destroyed.
RM178	Retain copies of all electronic aggregations and their records that have been transferred to The National Archives of Malaysia, at least until such time as a successful transfer is confirmed.[39] Any deletion before confirmation of a successful transfer is prohibited as provided for under Section 25(2), National Archives Act of 2003.
RM179	Have the ability to retain records management metadata for records and aggregations that have been destroyed or transferred.
RM180	Be able to export records in their native format or current format to which they have been migrated and in order of reference.
RM181	Be able to export all types of records which it is able to capture
RM182	Provide the ability to add user-defined records management metadata elements required for archival management purposes to electronic aggregations selected for transfer.
RM183	Provide the ability to sort electronic aggregations selected for transfer into ordered lists according to user-selected records management metadata elements.

Where hybrid aggregations are to be transferred, exported or destroyed, the electronic records management system **must**:

RM184	Require the administrator to confirm that the non-electronic part of the same aggregations has been transferred, exported or destroyed before transferring, exporting or destroying the electronic part.

3.6.3 Retention And Disposal Of Electronic And Non-Electronic Records

The electronic records management system **must**:

RM185	Support the allocation of records disposal schedule to every non-electronic aggregation in the classification scheme. The records disposal schedule must function consistently for electronic and non-electronic aggregations, notifying

---

[38] The Digital Archival Repository at The National Archives of Malaysia only accepts the XML format for metadata accompanying records transferred for permanent preservation.

[39] This is a procedural safeguard to ensure that records are not deleted before successful transfer is confirmed.

	the administrator when the disposal date is reached, but taking account of the different processes for disposing of electronic and non-electronic records.
RM186	Support the application of the same records disposal schedule to both the electronic and non-electronic aggregations that make up a hybrid aggregation.
RM187	Be able to apply any review decision made on a hybrid electronic aggregation to a non-electronic aggregation with which it is associated.
RM188	Alert the administrator to the existence and location of any hybrid non-electronic aggregation associated with a hybrid electronic aggregation that is to be exported or transferred.
RM189	Be able to record in the metadata all changes made to records management metadata references to non-electronic or hybrid aggregations and records.
RM190	Be capable of offering check-out and check-in facilities for non-electronic aggregations profiled in the system, in particular enabling the ability to record a specific user or location to which a non-electronic aggregation is checked out, and to display this information if the non-electronic aggregation is requested by another user.
RM191	Be capable of offering a request facility for non-electronic records profiled in the hybrid aggregation system, enabling a user to enter a date that the non-electronic element is required and generating a consequent message for transmission to the current holder of that non-electronic aggregation or the administrator, according to configuration.
RM192	Be able to export and transfer records management metadata of non-electronic records and aggregations.
RM193	Support the application of a review decision taken on a group of aggregations to any non-electronic aggregations within that group, by notifying the administrator of necessary actions to be taken on the non-electronic aggregations.

DISSEMINATE

3.7 Search, Retrieve And Render (Display)

Note that the electronic records management systems must never present information to any user who is not entitled to access it. All the features and functionality in this section must be subject to access controls as described in Section 3.4: Managing authentic and reliable records. To avoid complexity, this is assumed and is not repeated in each requirement below.

The electronic records management system **must**:

RM194	Provide a flexible range of functions that operate on the metadata related to every level of aggregation and on the contents of the records through user-defined parameters for the purpose of locating, accessing and retrieving individual records or groups of records and/or metadata.
RM195	Allow all record, volume and aggregation records management metadata to be searchable.
RM196	Allow the text contents of records (where they exist) to be searchable.
RM197	Allow the user to set up a single search request with combinations of records management metadata and/or record content.
RM198	Allow administrators to configure and change the search fields to:

	• specify any element of record, volume and aggregation records management metadata, and optionally full record content, as search fields; and • change the search field configuration.
RM199	Provide searching tools for: • free-text searching of combinations of record and aggregation records management metadata elements and record content; and • Boolean searching of records management metadata elements (see also Requirement 214).
RM200	Provide for 'wild card' searching of records management metadata that allows for forward, backward and embedded expansion.[40]
RM201	Allow searching within a single aggregation or across more than one aggregation.
RM202	Be able to search for, retrieve and display all the records and records management metadata relating to an electronic aggregation, or volume, as a single unit.
RM203	Be able to search for, retrieve and render an electronic aggregation by all implemented naming principles, including: • name; and • identifier (classification code).
RM204	Display the total number of search results on a user's screen and must allow the user to then display the results list, or refine the search criteria and issue another request.
RM205	Allow records and aggregations featured in the search results list to be selected, then opened (subject to access controls) by a single click or keystroke.
RM206	Allow users to retrieve aggregations and records directly through the use of a unique identifier.
RM207	Never allow a search or retrieval function to reveal to a user any information (records management metadata or record content) that the access and security settings are intended to hide from that user.
RM208	Have integrated search facilities for all levels of the classification scheme.[41]
RM209	Provide free-text and records management metadata searches in an integrated and consistent manner.
RM210	Present seamless functionality when searching across electronic, non-electronic and hybrid aggregations.
RM211	Allow users to save and re-use queries.
RM212	Allow users who are viewing or working with a record or aggregation, whether as the result of a search or otherwise, to see the record within the classification or aggregation hierarchy easily and without leaving or closing the record.[42]

---

[40] For example the search term 'proj*' might retrieve 'project' or 'PROJA'; the term 'C*n' would retrieve 'Commission'.

[41] In other words, users should see the same interface, features and options whether searching for classes, aggregations or records

[42] For example, when reading a record, the user should be able to see what volume and aggregation the record is associated with. If viewing aggregation records management metadata, the user should be able to find out

RM213	Allow users to refine (that is, narrow) searches.[43]

The electronic records management system **should**:

RM214	Provide word proximity searching that can specify that a word has to appear within a given distance of another word in the record to qualify as a search result (see also Requirements 197, 198 and 199).
RM215	Allow the records management metadata of any object (such as record, volume or aggregation) to be searched, whether the object itself is in electronic form or not, and regardless of whether the object is stored online, near-line or offline.
RM216	Provide display formats configurable by users or administrators for search results, including such features and functions as: • select the order in which the search results are presented; • specify the number of search results displayed on the screen; • set the maximum number of search results; • save the search results; and • choose which records management metadata fields are displayed in search result lists.
RM217	Provide relevance ranking of the search results.
RM218	Be able to relate an 'extract' of an electronic record to the original record, so that retrieval of one allows retrieval of the other, while retaining separate records management metadata and access controls over the two items.
RM219	Provide concept searches through the use of a thesaurus incorporated as an online index.[44]

Where a graphical user interface is employed, the electronic records management system **must**:

RM220	Provide a browsing mechanism that enables graphical or other display browsing techniques at any level of aggregation.[45]

3.7.1 Rendering: Displaying Records

The electronic records management system **must**:

RM221	Render or download records that the search request has retrieved.[46]
RM222	Render records that the search request has retrieved without loading the

information about the aggregation in which it is locate

[43] For example, a user should be able to start with the result list from a search and then initiate a further search within that list.

[44] This will allow retrieval of documents with a broader, narrower or related term in their content or records management metadata. For example, a search for 'ophthalmic services' might retrieve, 'health services', 'eye test' or 'ophthalmology'.

[45] This would be used with the searching techniques described above to provide a first-level view of records management metadata for a group of records or aggregations that have met the specified search criteria.

[46] If the electronic records management system is storing records in a proprietary application format, it may be acceptable for the rendering to be performed by an application outside the electronic records management system.

	associated application software.[47] The document viewer should be capable of displaying all the file formats in use in the public offices in Malaysia including the latest format such as MS Office 2007.
RM223	Be able to render all the types of electronic records specified by the organisation in a manner that preserves the information in the records (for example, all the features of visual presentation and layout produced by the generating application package), and which renders all components of an electronic record in their original relationship.[48]

3.7.2 Rendering: Printing

The electronic records management system **must**:

RM224	Provide the user with flexible options for printing records and their relevant records management metadata, including the ability to print a record(s) with records management metadata specified by the user.
RM225	Allow the printing of records management metadata for an aggregation.
RM226	Allow the user to be able to print out a summary list of selected records (for example, the contents of an aggregation), consisting of a user-specified subset of records management metadata elements (for example, Title, Author, Creation date) for each record.
RM227	Allow the user to print the results list from all searches.
RM228	Be able to print all the types of electronic records currently created by the public offices in Malaysia. Printing must preserve the layout produced by the generating application package(s) and include all (printable) components of the electronic record.
RM229	Allow the administrator to specify that all printouts of records have selected records management metadata elements appended to them, for example, title, registration number, date and security category.
RM230	Allow the administrator to print the thesaurus, where a thesaurus exists within the system.
RM231	Allow the administrator to print any and all administrative parameters.
RM232	Allow the administrator to print records disposal schedules.
RM233	Allow the administrator to print the classification scheme.
RM234	Allow the administrator to print metadata schema or element sets
RM235	Allow all records in an aggregation to be printed, in the sequence specified by the user, in one operation.
RM236	Allow the administrator to print the file list.

3.7.3 Rendering: Redacting Records

A redacted record is a copy of an electronic record from which some material has been removed or permanently masked (redacted). An extract is made when the full record cannot be released for access, but part of the record can.

---

[47] This is typically provided by integrating a viewer software package into the electronic records management system. This is frequently desirable to increase speed of rendering.

[48] The organisation must specify the application packages and formats required.

The electronic records management system **must**:

RM237	Allow the administrator to take a copy of a record for the purposes of redaction.[49]
RM238	Record the creation of extracts in the records management metadata, including at least date, time, reason for creation and creator.
RM239	Store in the metadata any change made in response to the requirements in this section.
RM240	Provide functionality for redacting (see Glossary at Appendix 2) sensitive information from the extract. If the electronic records management system does not directly provide these facilities, it must allow for other software packages to do so.[50]
RM241	Prompt the creator of an extract to assign it to an aggregation.
RM242	Store a cross-reference to an extract in the system.

3.7.4 Rendering: Other

This section applies only to records that cannot meaningfully be printed, such as audio, visual and database files.

The electronic records management system **must**:

RM243	Include features for rendering those records that cannot be meaningfully printed to an appropriate output device.[51]

3.7.5 Rendering: Re-Purposing Content

The electronic records management system **must**:

RM244	Allow the re-use or re-purposing of content.[52]

ADMINISTER

3.8   Administration

In exceptional circumstances, records may be altered or deleted by system administrators. Where this is the case, copies of the records without the sensitive information (redacted copies) must be able to be created. System administrators also need to be able to manage system parameters, back up and restore data, and generate system reports. This section includes requirements for managing system parameters,

---

[49] This copy is referred to as an 'extract' of the record in this requirement (see Glossary at Appendix 2).

[50] It is essential that when these or any other reduction features are used, none of the removed or masked information can ever been seen in the extract , whether on screen, printed or played back regardless of the use of any features such as rotation, zooming or any other manipulation.

[51] Examples include audio video and some websites.

[52] An example may be allowing the user to cut text from a word-processed record or appending a dynamic link to an image-based record within another context.

back-up and restoration, system management and user administration. The administration of security classification, controls, classification and so on are addressed in the relevant security-related requirements in Section 3.4: Managing authentic and reliable records.

3.8.1 Administrator functions

The electronic records management system **must**:

RM245	Allow the administrator to retrieve, display and re-configure system parameters and to re-allocate users and functions between user roles.
RM246	Provide back-up facilities so that records and their records management metadata can be recreated using a combination of restored back-ups and metadata.
RM247	Provide recovery and rollback facilities in the case of system failure or update error, and must notify the administrator of the results.[53]
RM248	Monitor available storage space and notify the administrator when action is needed because available space is at a low level or because it needs other administrative attention.
RM249	Allow the administrator to make bulk changes to the classification scheme, ensuring all records management metadata and metadata data are handled correctly and completely at all times, in order to make the following kinds of organisational change: • division of an organisational unit into two; • combination of two organisational units into one; • movement or re-naming of an organisational unit; and • division of a whole organisation into two organisations.[54]
RM250	Support the movement of users between organisational units.
RM251	Allow the definition of user roles, and must allow several users to be associated with each role.
RM252	Communicate errors encountered in storing data

3.8.2 Metadata Administration

Metadata schemas have to be administered, including the creation, addition, deletion or alteration of metadata elements, and the semantic and syntactical rules and obligation status applied to those elements.

---

[53] That is, the electronic records management system must allow administrators to 'undo' a series of transactions until a status of assured database integrity is reached. This is only required when error conditions arise.

[54] When such a change is made, closed files must remain closed, retaining their references to the classification scheme before the change, and open files must either be closed, retaining their references to the classification scheme before the change and cross-referenced to a new file in the changed scheme, or be referenced to the changed scheme, but clearly retaining all prior references to the classification scheme before the change. Changes to organisational units described above may imply corresponding changes to the classification schemes of the units and their user populations. The term 'bulk changes' implies that all aggregations and records affected can be processed with a small number of transactions, rather than needing to be processed individually. Note that this element will apply especially where classification schemes are based on an organisation plan and be less necessary where classification is functionally assessed.

The electronic records management system **must**:

RM253	Allow the administrator to create, define and delete metadata elements, including custom fields.
RM254	Allow the administrator to apply and modify metadata schema rules, including semantic and syntactical rules, encoding schemes and obligation status.
RM255	Allow the administrator to configure the system to restrict the viewing or modifying of metadata elements by group, functional role or user.
RM256	Document all metadata administration activities.

3.8.3 Reporting

This section articulates basic reporting requirements. It does not articulate the requirements for a comprehensive reporting subsystem.

The electronic records management system **must**:

RM257	Provide flexible reporting facilities for the administrator. They must include, at a minimum, the ability to report the following: • numbers of aggregations, volumes and records; • transaction statistics for aggregations, volumes and records; and • activity reports for individual users.
RM258	Allow the administrator to report on metadata based on selected: • aggregations; • volumes; • record objects; • users; • time periods; and • file formats and instances of each format.
RM259	Be able to produce a report listing aggregations, structured to reflect the classification scheme, for all or part of the classification scheme.
RM260	Allow the administrator to request regular periodic reports and one-off reports.
RM261	Allow the administrator to report on metadata based on selected: • security categories; • user groups; and • other records management metadata.
RM262	Include features for sorting and selecting report information.
RM263	Include features for totalling and summarising report information.
RM264	Allow the administrator to restrict users' access to selected reports.

3.8.4 Back-Up And Recovery

Electronic records management systems must have comprehensive controls to create regular back-ups of the records and records management metadata that they maintain. These back-ups should enable the electronic records management system to rapidly recover records if any are lost because of system failure, accident or security breach. In practice, back-up and recovery functions may be divided between electronic records management system administrators and IT staff.

The electronic records management system **must**:

RM265	Provide automated back-up and recovery procedures.
RM266	Allow the administrator to schedule back-up routines by: • specifying the frequency of back-up; and • allocating storage media, system or location for the back-up (for example, offline storage, separate system, remote site).
RM267	Allow only the administrator to restore from electronic records management system back-ups. Full integrity of the data must be maintained after restoration.
RM268	Allow only the administrator to roll-forward the electronic records management system from a back-up to a more recent state, maintaining full integrity of the data.
RM269	Allow users to indicate that selected records are considered to be 'vital records'.[55]
RM270	Be able to notify users whose updates may have been incompletely recovered, when they next use the system, that a potentially incomplete recovery has been executed.

3.9   Multimedia Repository

Multimedia Repository (MR) is a repository system that will store any multimedia resources, which are not necessarily related to records in other modules (e.g. minutes of meetings, planning papers, etc.). The repository should support all media types, including images, videos, audios, word processing documents, spreadsheets, and presentations, in fact, any on-line, near-line or off-line resource.

3.9.1 Content Creation

The electronic records management system **must**:

RM271	Allow Asset Management and allow multiple users to edit content and make changes
RM272	Have Editing Tools such as text based editor with spell-check capabilities; ability to consolidate changes from multiple editors; ability to edit within the system as well as external to the system (i.e., in MS Word). If editing is to be done within original application, the application should be integrated with the CMS.
RM273	Allow Multiple Content Sources: Text; Graphic; Database; Multimedia or other. Please name it.
RM274	Have Creation Templates as well as the ability to use standard and customized templates for content creation within system.
RM275	Have Publishing Templates with standard templates for presentation of material available, as well as ability to customize.
RM276	Have Word Templates and accommodate storage, display of MS Word or other Templates. Please name it.

---

[55] Vital records are those records that are absolutely necessary for the organisation's ability to continue its business either in terms of its ability to cope with emergency/disaster conditions or to protect its financial and legal interest. The identification and protect its financial and legal interests. The identification and protection of such records, therefore, is of great importance to any organisation.

RM277	Enable Content Creation such as ability to generate PDF format as needed.
RM278	Have Check-in/Check-out Feature with the ability to check content/document out for editing, ability to track who has documents checked out and block editing of same document already in edit mode.
RM279	Enable separation of Content and Presentation such as the ability to separate the creation and presentation of content through use of templates.
RM280	Enable Content Reuse - ability to reuse content in multiple templates/documents
RM281	Have Collaboration System Features - allow users to work together on content/document
RM282	Enable comments to be attached to specific text - ability to attach comments during the editing process to specific areas of text as well as to the document as a whole.
RM283	Enable archiving of content.
RM284	Allow Version Control - application of version control by content creator, save past versions in system so that can roll back if necessary, track date and time of changes and ability to keep comment log.
RM285	Enable tracking of changes between versions and ability to identify and compare changes between document versions.
RM286	Allow self-service authoring for non-technical content providers: Content authors should be able to quickly create materials using standard desktop applications.

3.9.2 Workflow

The electronic records management system **must**:

RM287	Have integration-messaging - integration of other channels of communication into workflow, i.e., email notifications.
RM288	Have workflow process - ability to define multiple steps involving various content types, cross-departmental staff and required actions, include triggers by date (automatic notification to update or archive content) and by actions (creation, deletion, editing, etc.)
RM289	Allow parallel and sequential workflow - ability to allow multiple users to edit content at the same time, and also provide a sequential based workflow.
RM290	Allow workflow queues - with ability to show what content is in what state for a particular user id and what content is in what state for groups of users.
RM291	Allow comments – ability to attach comments to a workflow stage.

3.9.3 Metadata and Search

The electronic records management system **must**:

RM292	Enable metadata management - must have a native or integrated metadata management tool, ability to change and add metadata fields, conduct global search and replace content for metadata fields and have ability to export metadata lists.
RM293	Permit thesaurus support – accommodate use of predetermined thesaurus/controlled vocabulary during search.

RM294	Enable cross-references - system must support a cross-reference or synonym function to relate terms from thesaurus.
RM295	Provide drill down interface based on hierarchy.
RM296	Allow limited search - ability to limit scope of search functions to selected topics from hierarchy (combines drill down and search functionality).
RM297	Allow fuzzy searching - ability to recognize misspellings and to suggest alternatives
RM298	Allow attribute searching - ability to search metadata as well as provide text word searching (therefore metadata must be stored in such as way as to accommodate search engine access).
RM299	Allow Administrator to control taxonomy (Designed hierarchy of topics and thesaurus controlled by the administrator and not changeable by users).
RM300	Support Taxonomy (multiple hierarchies for documents) - topics maybe repeated within hierarchy and documents may be linked to multiple locations.
RM301	Provide access to external information sources – with ability to provide links to external websites and print content that has listing within the system, i.e., through a catalog.
RM302	Have ability to relate documents within system.

3.9.4 User Interface

The electronic records management system **must**:

RM303	GUI Administration features: All configurations, setup, scheduling and other admin functions accessible through a GUI.
RM304	Customizable interface: Ability to customize the user interface as needed.
RM305	Personalization: Personalize according to user group roles, i.e., internal searcher, external searcher, editors

The electronic records management system **should**:

RM306	Be Browser based - use web based interface for user access to system.

3.9.5 Reporting & Administration

The electronic records management system **must**:

RM307	Have reporting tools - include performance, workflow, log file analysis; session analysis and ability to create custom reports as needed.
RM308	Have audit trail - provide audit trails for system activity, including workflow and revision history.
RM309	Provide content caching to provide better response time.

The electronic records management system **should**:

RM310	Provide automatic link checking and validation for internal and external links.

3.9.6 Security

The electronic records management system **must**:

RM311	Have role based security - provide security according to user role (Combine with document level security to accommodate different editing/author teams).
RM312	Have document level security - allow security to the document level.
RM313	Allow integrated authentication - provide a user authentication mechanism. (Active Directory integration preferred).
RM314	Have compatibility with security technology, for example SSL.

3.10   Enterprise Content Management

A content management system (CMS) supports the creation, management, distribution, publishing, and discovery of the records. It covers the complete lifecycle of the pages on the system, from providing simple tools to create the content, through to publishing, and finally to archiving. It also provides the ability to manage the structure of the system, the appearance of the published pages, and the navigation provided to the users.

3.10.1 All Software Modules

The electronic records management system **must**:

RM315	Have a general release date for all software modules of the proposed CMS solution prior to the date of the supplier proposal.
RM316	Prompt for document metadata - The system shall prompt the user for document metadata at the time of creating, saving or closing a document and at the time of sending an e-mail.

3.10.2 Architecture

The electronic records management system **must**:

RM317	Support a three-tiered architecture - the logical and physical separation of metadata storage from document repository storage, and the separation of client processes, server processes and interfacing processes.
RM318	Support the creation of multiple, distributed repositories and transparent access to multiple, distributed document repositories from any client.
RM319	Have a highly integrated product architecture with tightly integrated back-end application server.
RM320	Be scalable to the number of users, retrieval volume and document storage (provide method of sizing used in determining the CMS platform).
RM321	Support access to repositories and workflow functionality over the Internet and intranet (WAN and LAN).
RM322	Support the estimated volume of transactions and documents through features such as server replication and clustering or equivalent.
RM323	Support fail-over back-up and recovery capabilities.
RM324	Support various data storage platforms. Please name.
RM325	Support RDBMS. Please name.

3.10.3 Desktop Client

The electronic records management system **must**:

RM326	Support Windows NT and WIN 2000 and above clients.
RM327	Support access to the document repositories and workflow functionality through Internet Explorer, Netscape Navigator and other industry-standard browsers.

3.10.4 Security / Access

The electronic records management system **must**:

RM328	Support very granular access and security restrictions, including the creation of groups of users with specific document manipulation rights (add documents, delete, view, print, etc.) to designated types of documents (index field) groups of documents (index field) and specific individual documents.
RM329	Be configurable at the case file (collection of documents) and document (multiple pages) levels.
RM330	Permit the security/access restrictions on documents and groups to be modified, and to add/delete members to/from a group.
RM331	Be configurable for a single individual, multiple specific users, all users and other membership parameters.
RM332	Allow a user to belong to more than one group for purposes of document access and hide from view the existence of any documents the current user is not permitted access to.

3.10.5 Image Capture

The electronic records management system **must**:

RM333	Support appropriate scanners for the page volumes, but the scanners must be capable of scanning a minimum of 25 ppm.
RM334	Support the following file formats/compression formats: TIFF multi-page files G3 and G4 compression, JPEG, GIF, XML, PDF, WAV, MP3, MPEG, AVI.
RM335	Support the deletion and re-scanning of pages/documents before committing to disk.
RM336	Support various image enhancement and clean-up techniques such as de-skew, de-speckle and darkening/lightening.
RM337	Support image capture at different dpi.
RM338	Support bi-tonal and gray-scale image scanning and if possible color scanning too.
RM339	Support imaging of 8-1/2" x 11", legal size, single-sided or double-sided pages (duplex on demand).

3.10.6 Image Capture Indexing

The electronic records management system **must**:

RM340	Support automatic indexing through barcode recognition for interleaved 3 of 9.

3.10.7 Document Management

The electronic records management system **must**:

RM341	Support a hierarchical organization of documents in folders (files).
RM342	Support multiple formats of documents in a single folder.
RM343	Be able to produce an audit trail for various document activities such as add, delete, view, print, etc.
RM344	Support concurrent read/print access to documents by multiple users.
RM345	Provide the capability to restrict document manipulation functions (add, delete, modify) to certain users based on user-selectable parameters (e.g., case type and document type).
RM346	Support digitally signed objects.
RM347	Have the capability to rendition documents from MS Word to PDF format or others. Please name.
RM348	Provide the capability to any user to view or "play" any electronic object types stored in the repository.
RM349	Provide convenient page viewing features such as rotate, zoom, go to "n" page; book marks, etc.
RM350	Support XML documents or other formats. Please name.
RM351	Provide creation, viewing and printing of annotations on documents, pages and folders.
RM352	NOT store annotations in image headers.

The electronic records management system **should**:

RM353	Be able to catalog documents that are stored off-line.
RM354	Restrict access to annotations to authorized users.

3.10.8 Records Management

The electronic records management system **must**:

RM355	Provide automatic migration of documents between storage platforms as part of the archiving and document lifecycle management process based on triggering events initiated from another system.

3.10.9 Workflow

The electronic records management system **must**:

RM356	Support rules-based production workflow routing to process documents through electronic queues.
RM357	Support split screen viewing (a document in one window and another application screen in a second window).
RM358	Provide the capability of routing documents based on user decisions.
RM359	Maintain a log of actions that have been taken on a document (e.g. the routing sequence, notes about problems in processing a document, people who need to review the document and other annotations).
RM360	Support a "universal inbox" which is accessible concurrently by multiple users and secure inboxes (access restricted to specific users).
RM361	Support the generation of workflow statistics and status of work items reports.

RM362	Support conditional (if .. then …) logical routing and rendezvous (wait for another action to occur before processing document to a work queue).
RM363	Support parallel routing (routing for the same document to more than one inbox at the same time).
RM364	Be able to be accessed and executed over the intranet, via dial-up access and over the Internet by browser-based clients.
RM365	Be able to be created by trained end-users through graphical tools, using such techniques as "drag and drop".
RM366	Support inter-agency workflow processes.

3.10.10 System Administration

The electronic records management system **must**:

RM367	Use graphical tools.
RM368	Have Operating Systems with services such as User IDs, passwords and security levels (for example Windows, Linux etc).
RM369	Enable remote systems administration over an intranet.

3.10.11 Fax

The electronic records management system **must**:

RM370	Be capable of importing and exporting documents to/from the document repository.

3.10.12 Printer

The electronic records management system **must**:

RM371	Have high volume and high speed print capabilities to cater to the needs of the agency.
RM372	Be able to send print jobs to network printers and to print from individual printers attached to workstations.

3.10.13 Web Publishing

The electronic records management system **must**:

RM373	Be able to send print jobs for web publishing to network printers and to print from individual printers attached to workstations.
RM374	Allow browser-based users to enter information over the Internet into forms, and for forms-based information to propagate through the system using the product's workflow or other capabilities.
RM375	Facilitate browser-based users to search for and retrieve, download and print documents in the repository.

3.10.14 System

The electronic records management system **must**:

RM376	Support mirrored drives.
RM377	Include back-up capabilities for the document repository and database(s).
RM378	Be Year 2000 Compliant and free from any date-related malfunctions.

3.11 Collaboration Management

Collaboration System (CS) Requirements

3.11.1 Correction and Creation

The electronic records management system **must**:

RM379	Allow the users to create new documents and edit existing documents.
RM380	Provide a central secure document repository for storing all the created documents.
RM381	Version control – The user shall have the option whether to create a new version, replace the existing version (provided the document has not been finalized) or create a new document. New versions shall be automatically linked to the original document and higher or lower versions of the document.
RM382	Linking document attachments - The user is able to attach/link multiple electronic documents to form a single "virtual document" which is subsequently managed as a single entity to ensure its integrity.
RM383	Profiling documents with attached images – The user shall be able to profile an original hardcopy document and to attach its image as electronic attachments.
RM384	Launching of applications – The system shall launch the authoring applications (i.e. associated or generic viewer) from within the document retrieval function of the Collaboration System for the purpose of creating, editing or viewing a document.

3.11.2 Instant Messaging

The electronic records management system **should**:

RM385	Secure communication (including message encryption)
RM386	Support Instant Messaging clients
RM387	NOT support desktop client software beyond a standard web browser
RM388	Give the user the capability to present documents to session participants through their browser.
RM389	Have the capability to identify the status of the team members, whether they are "Away", "Out to Lunch", "Busy" or "On the Phone". (This enables users to see instantly the availability of other Team Members in joining the conference / Meeting)
RM390	Instantly escalate Instant Messages to conferences and web Collaboration sessions

3.11.3 Paging

The electronic records management system **must**:

RM391	Provide the capability for multiple users to collaborate together in a single session simultaneously.
RM392	Allow users to leave and rejoin sessions.
RM393	Provide the capability for the users to schedule and hold online meeting with identified team members / participants.
RM394	Automatically alert or send notifications to users on the meeting schedules.

The electronic records management system **should**:

RM395	Be able to display presentation slides for other participants during the online meeting through shared web browser (Communication with other participants is provided through audio/video links and chat application).
RM396	Provide whiteboard tools that can be used to clarify meeting issues.
RM397	Allow users the option to share their screens or selected applications. (All users have access to the list of meeting participants)

3.11.4 Security

The electronic records management system **must**:

RM398	Provide an individual profile for each Collaboration System user and a facility for managing "permission" associated with read, write, modify, delete and disposal rights and restrict those permissions to designated individuals at the group, document and file classification level.
RM399	Allow the user to electronically designate a document as being finalized (authorized by a named authority) thereby protecting the document from modification.
RM400	Enable administrator and records manager to restrict creation of new files to designated users.
RM401	Provide a strong encryption feature for meeting the requirements for handling Government classified information.
RM402	Have its own self-contained security system and protect the integrity of information within the system throughout each stage of the life cycle of the record.
RM403	Provide an audit log showing changes made to the security parameters.
RM404	Protect against unauthorized access by hiding from the end user, the user ID and password information used for access and prevent unauthorized access to all system tables.
RM405	Use the same password facility as the LAN and must not impose the use of additional passwords to gain access to the system.

3.11.5 Retention and Disposal

The electronic records management system **must**:

RM406	Be able to create, maintain, modify and manage retention and disposal schedules indicating the period of time documents are to be retained in an active and inactive state; and to create, maintain, modify and manage a listing with instructions for the authorized Disposal of documents such as destruction or transfer to the National Archives of Malaysia.
RM407	Enable administrator and Records Manager to change defaulted retention and disposal designations for individual documents in order to support disposal exceptions.
RM408	Provide on-line assistance and an enabling mechanism to change document status between active, inactive and archival storage.
RM409	Provide a means to identify all official documents due for destruction, within the workgroup according to their authorized records disposal schedules.
RM410	Provide a means to delete a document and its attachments from all repository media (including removable media) such that the document and its attachments

	cannot be reconstructed if such deletion is authorised by the National Archives of Malaysia under Section 25 of the National Archives Act 2003.

3.11.6 Retrieval

The electronic records management system **must**:

RM411	Bookmark frequently used / common documents.
RM412	Enable the user to select one or more document repositories prior to invoking a document search and to present the search results from the selected repositories in a combined manner showing the source repository.
RM413	Enable the user to use intelligent search, such as Boolean and fuzzy search to search on document contents. All searching shall be case insensitive as default, while also allowing case-sensitive searches.
RM414	Provide facilities to ensure that "read, write and modify rights" are restricted to designated individuals for department-wide repository access rights.

3.11.7 Thesaurus search

The electronic records management system **must**:

RM415	Enable users to perform thesaurus searches on the document contents using either the English or Bahasa Malaysia interface.
RM416	Provide the ability to select a term in either Bahasa Malaysia or English. A single search would then be performed using the terms provided.

3.11.8 Retrieval Presentation

The electronic records management system **must**:

RM417	Provide a facility to retrieve electronic documents and associated attachments from any document repository (or a collection of documents) informing user on location of document (e.g. online, offline, etc.)
RM418	Include the capability to view electronic documents without launching the native or originating application.
RM419	Allow the user to view, retrieve or print electronic documents from a customizable hit list.
RM420	Enable the user to select and retrieve one or more documents from an attached/linked multiple electronic documents (a single "virtual document").
RM421	Provide a mechanism to ensure that the default retrieval strategy shall always retrieve only the most recent version of a document. The system must also provide a facility for the retrieval of any or all earlier versions of an electronic document as requested by the user.
RM422	Provide each user with a list of the most recently edited or profiled documents at the desktop.

3.11.9 Check-in/ Check-out and Editing of Electronic Documents

The electronic records management system **must**:

RM423	Enable the user to check-in and check-out electronic documents.
RM424	Prevent other users from modifying a checked-out document but allow viewing

	access by those users.
RM425	Provide notification, when a user attempts to access a file that has been checked-out.
RM426	Provide the capability to check-in a document without having to launch the native application.
RM427	Allow the administrator to specify a default "application, and its version, of choice" for editing sessions, where a file format is supported by multiple applications (e.g. *.BMP is supported by a number of graphics editors).
RM428	Provide the capability to open additional documents into an existing instance of an application

3.11.10 Auditing

The electronic records management system **must**:

RM429	Maintain charge in / out history for files, volumes, documents and secondary storage containers.
RM430	Provide the capability to compile statistics and produce management information such as the number of times a document is accessed/processed/updated as well as the number of documents accessed by organizations/groups.
RM431	Maintain and provide reports on revisions to document, access to document and change to document status.

3.11.11 Interface

The electronic records management system **must**:

RM432	Provide a Graphical User Interface (GUI) interface or a web-enabled interface.
RM433	Enable a designated individual to access, revise or make additions to online help facilities including the capability to load, maintain and retrieve custom process rules pertaining to using and administering the Collaboration System.

3.11.12 Workflow

The electronic records management system **must**:

RM434	Have the capability to route the information to specific participants before posting it for general consumption and can be used to indicate when and where that information will be posted.

3.11.13 Email System

The electronic records management system **must**:

RM435	Allow integration with messaging software such as Lotus Notes. The user shall be able to (a) Transfer e-mail messages, their associated documents and attachments between messaging software such as Lotus Note and the system such that e-mail messages can be filed in an Collaboration System repository; and initiate mailing Collaboration System-filed documents from a Collaboration System repository as attachments to an e-mail message.

RM436	Provide a facility for automatically capturing e-mail message attachments (sent and received).
RM437	Use document name and not system generated name that may or may not be arbitrary filename for the capture of emails and email attachments (for example John Smith and not foxman@domain).

3.11.14 Replication

The electronic records management system **must**:

RM438	Provide the capability for users to work with the document offline and synchronize automatically when the users are online.
RM439	Enable replicated repositories – the technical architecture provides replicated repositories, which are duplicates of a repository that can be distributed to different geographical locations.

3.11.15 Knowledge Management

The electronic records management system **must**:

RM440	Have the capability to support the concept of a "group memory". (Store the intellectual capital and can be reuse by other users).
RM441	Have the capability to reuse the knowledge and best practices adopted by the users in the Collaboration System.
RM442	Bookmark for frequently used knowledge and best practices adopted by the users in the Collaboration System.

3.11.16 Tracking

The electronic records management system **must**:

RM443	Provide the capability for the users to view and track the status and milestones of the task.
RM444	Provide the capability to alert and notify the users regarding the expiring of due date.

3.11.17 Multimedia Support

The electronic records management system **must**:

RM445	Provide the capability to support for MPEG, JPEG, AVI, Flash TM QuickTime TM, GIF, WAV, AU and MS Windows bitmap etc.

3.11.18 Virtual Briefcase

The electronic records management system **must**:

RM446	Provide a virtual workplace / environment for users to view, edit and create information / documents.
RM447	Provide a "virtual room" construct to provide multiple shared virtual spaces for collaborative use of researching, planning, communications and analysis tools.

3.11.19 Additional Functional Requirements

The electronic records management system **must**:

RM448	Provide the capability for users to add in comments / suggestions to the working documents. (Only for authorized users)

3.11.20 Notification Process *delivers real-time alerts of significant enterprise events via remote notification technologies, such as cell phones, electronic mail, and other custom notification techniques*

The electronic records management system **must**:

RM449	Allow users to send messages in respond to various events during a process. For example, ability to notify a system operator if the process fails or e-mail a report produced by the process if it succeeds.
RM450	Enable the format for the email notification to include the title of the event.
RM451	Notify the respective team members regarding an expired deadline or if a workflow was fulfilled successfully through a triggered notification process.
RM452	Categorize email notifications into at least two categories such as Urgent email and Normal email.
RM453	Ensure that the notification system is easy to use, has a point and click interface, and can be used to define notification escalation chains. When an action fires, the notification will continue to escalate at the specified time intervals, until the desired individual responds to the event.

The electronic records management system **should**:

RM454	Allow the users to customize their notification and provide details of every aspect of the notification process and historical reporting for use in capacity planning.
RM455	Be able to offer a wide range of options for sending status messages for the process, including the ability to send files produced by the process.

PRE-REQUISITES FOR ERMS IMPLEMENTATION

Agencies are required to develop their **E-file Plans** and **Records Disposal Schedules** which are pre-requisites for ERMS implementation. An agency would have to prepare its E-file Plan and Records Disposal Schedule and have it approved by the National Archives of Malaysia as required by The National Archives Act of 2003 before it can be inbuilt into the ERMS system. Agencies can seek advice and help from the National Archives of Malaysia in developing both these pre-requisites.

Preparation of the E-file Plan and the Records Disposal Schedule needs good planning and execution. It also requires commitment from top level management as it is pertaining to the management of one of its most prized and valuable asset which if mismanaged or lost can cause the organisation to be crippled.

The e-file Plan and Records Disposal Schedule is prepared after assessment of the functions and activities of the agency as well as appraisal of the value of the records created by the agency.

Appraisal Management

The Appraisal Process is the process whereby electronic records are assessed to determine whether or not the electronic records have archival value. The assessment of the electronic records will be based on Arkib Negara Malaysia's pre-defined criteria, as well as the public office's specific requirements.

For the current practice in conventional records, appraisal is mainly done at the 'series or file level'. This is because, a document by itself may not have the archival value but it may provide the context that links the rest of the document in that particular file or series. As such it is important to note that with electronic records the same applies. I.e. the electronic records will be appraised at the 'series or folder' level as opposed to the document or individual electronic files. If a series or folder has been classified to be archival value, any items or electronic files that are stored or saved into that folder will be archived according to the determined disposal schedule.

It is also important to note that the appraisal process is the responsibility of Arkib Negara Malaysia and the public office. The appraisal at the public office is even more critical as this is where electronic records that have archival value are first identified.

The appraisal process will have to be conducted at point of creation and capture.
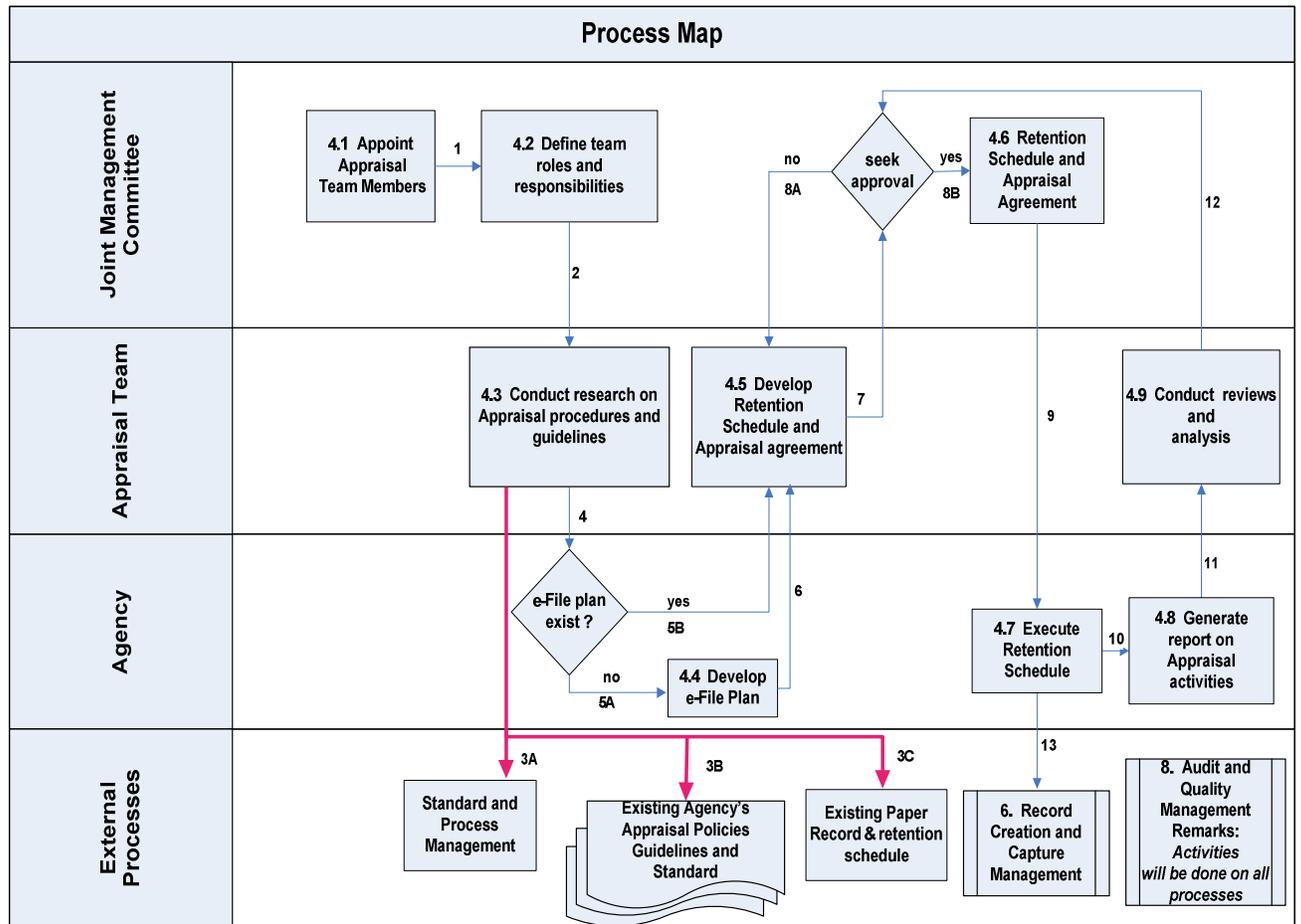
APPRAISAL MANAGEMENT

Figure 4: High Level Business Process for Appraisal Management

Description of the Business Process:

1.   4.1 Appoint Appraisal Management team members: A series of activities to identify and appoint the person involved in planning and executing the Appraisal Management activities.

2.   4.2 Define team roles and responsibilities: To define the roles and responsibilities of the Appraisal Management to its members and to define their roles and responsibilities as a team for the effective execution of any Appraisal activities.

3   4.3 Conduct study on Public Office's Record Management environment: A series of ongoing activities to acquire knowledge, experience and lessons learned, new methods and best practices in the Public Office Records Management.

4.   4.4 Develop e-File plan: The activity of determining the file location to place an electronic record.

5.   4.5 Develop Retention Schedule and Appraisal Agreement: A series of activities to identify and document the retention period of a record into an executable schedule.

6.   4.6 Retention Schedule and Appraisal Agreement: A legal document that binds ANM and the Public Office with respect to the details of the Retention schedule and Records Appraisal process.

7.   4.7 Execute Retention Schedule and Appraisal Agreement: A series of activities to implement the retention schedule and the appraisal activities as agreed in the Appraisal Agreement.

8.   4.8 Generate reports on Appraisal activities: To generate the Appraisal Report, the activities involved are to determine the report format, identify the target audience and the information to be reported and the frequency of the report.

9.   4.9 Conduct review and analysis: To conduct a series of analysis on the review and feedback so that any new recommendations and issues arise from the implementation of the Appraisal methods are addressed and acknowledged for improvement.
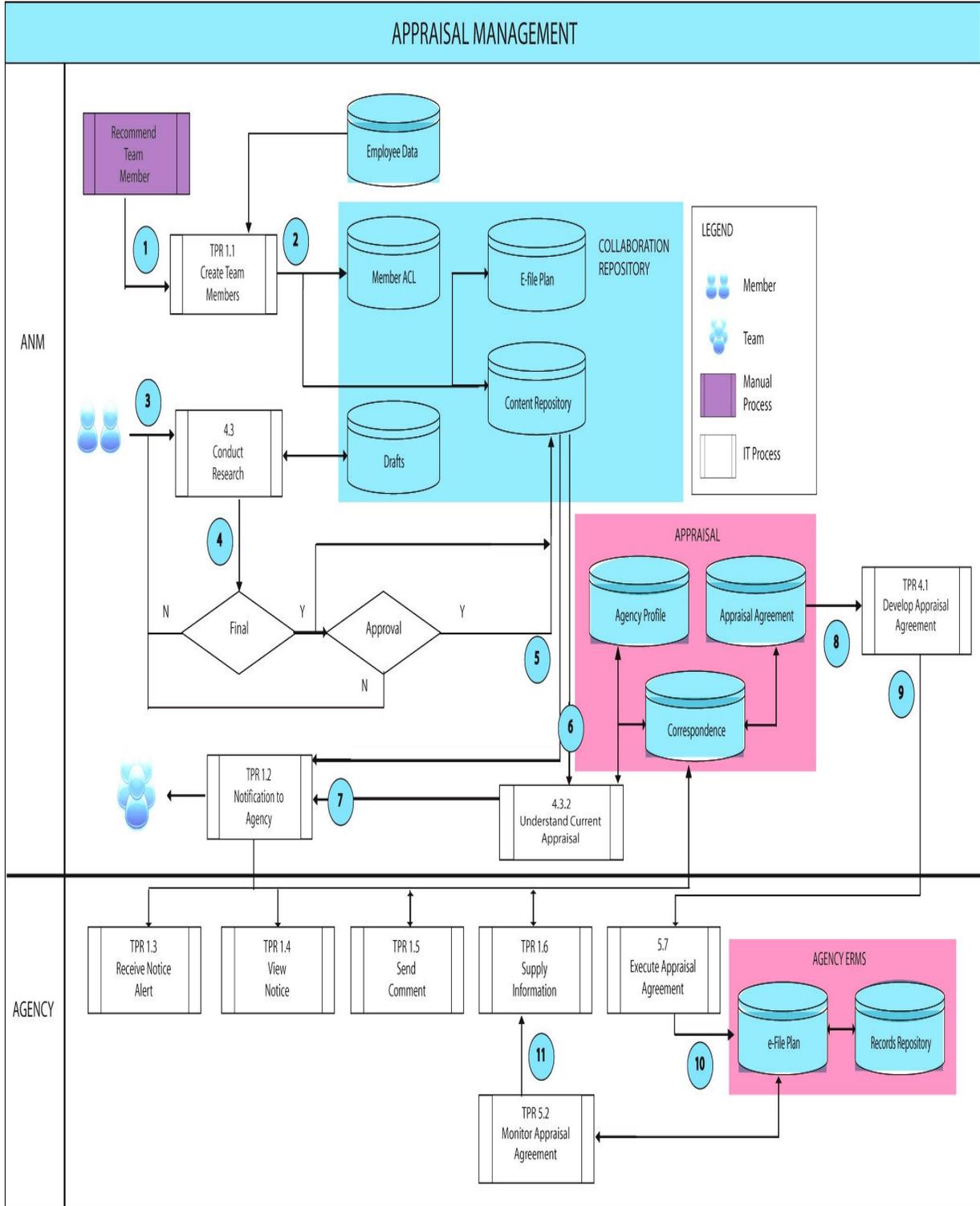
IT PROCESS FLOW

Figure 5: IT Process Flow Chart

Description of the IT Process Flow:

(a).   The administrator will create the team based on the recommended team members provided by the unit's management. This process will create

- Member Action Control list based on any existing employee data mapped against the role of the member
- e-File Plan to store the various rules related to the content including workflow and process flow
- Draft repository for the content to allow team members a shared area to store their respective work-in-progress
- Content Repository to host the various contents that is approved for Distribution

(b).   The administrator will sign-off the various workflow and processes flow to the various team approval committee.

(c).   Team Members start creating content and work on the content in the shared drive repository.

(d).   When the content is ready for distribution, and the team member declares the content as a record, the application will check across the e-file plan for the content file plan i.e. whether the content requires an approval for distribution.

(e).   Once the publication is ready for distribution, the respective ANM group will publish a circular to notify Public Offices of this new update. This is performed through the BPR 2.5 processes. There will be an automated process that moves this content over to the publication area.

(f).   Once the content is ready for publication, the respective ANM group will publish a circular to notify Public Offices of this new update. This is performed through the BPR 5.3 processes. There will be an automated process that moves this content over to the publication area.

(g).   Once the notification is sent out, the system will allow the Public Offices to view their respective correspondence provided through the notification module. This system allows the Public Offices to perform the following functions.

- Review the correspondence, notices, circulars for the Public Office's consumption
- The Public Offices are also allowed to send their comments or queries to ANM. This will then be routed to the respective personnel in-charge

(h).   Once the base information is available, ANM will schedule time to develop the appraisal agreement with the Public Office. The appraisal agreement will allow both parties to confirm and populate the templates for:

- Record
  - Classes
  - Classification
  - Life Cycle

- e-File Plan
  - Retention Schedule
  - Vital Record Rule
  - Permanent Record Rule
  - Disposal Rule
  - Packaging Rules

(i).   Once the Appraisal Agreement is approved, ANM will transfer the agreement to the Public Office.

(j).   The Public Office will then execute the agreement. This module will generate the e-file plan and records repository based on the records definition and classification for the Public Office.

(k).   The Public Office will monitor all activities related to the agreement. This includes all new creates, updates and deletions of the agreement components. Based on any new activity notification and information will be supplied to the ANM monitoring system for updates.

GLOSSARY

Term	Definition
Access	The right, opportunity, means of finding, using or retrieving information. Source: ISO 15489, Part 3, Clause 3.1.
Access controls	A scheme of non-hierarchical mechanisms, which may be applied to digital records to prevent access by unauthorised users. May include the definition of user access groups and ad hoc lists of individual named users. See also **Security controls, System access control** and **User access group**. Source: Adapted from The National Archives (UK), *Requirements for Electronic Records Management Systems, 3: Reference Document*, 2002, p. 28.
Accountability	The principle that individual, organisations and the community are required to account to others for their actions. Organisations and their employees must be able to account to appropriate regulatory authorities, to shareholders or members, and to the public to meet statutory obligations, audit requirements, relevant standards and codes of practice, and community expectations.
Acquisition	The act of receiving records from one organization and transferring custody and processing of those particular records to the receiving organization.
Acquisition Management	The area of management where records acquisition is planned, executed and monitored; to ensure compliance to the Arkib Negara Malaysia Act for the purpose of preservation.
Action tracking	The process in which time limits for actions are monitored and imposed on those conducting the business
Activity	The second level of a business classification scheme. Activities are the major tasks performed by an organisation to accomplish each of its functions. An activity is identified by the name it is given and its scope note. The scope of the activity encompasses all the transactions that take place in relation to it. Depending on the nature of the transactions involved, an activity may be performed in relation to one function, or it may be performed in relation to many functions. See also **Business classification scheme**, **Function** and **Transaction**.

Term	Definition
Adequate	Records should be adequate for the purposes for which they are kept. Thus, a major initiative will be extensively documented, while a routine administrative action can be documented with an identifiable minimum of information. There should be adequate evidence of the conduct of business activity to be able to account for that conduct.
Administrator	A role responsible for the day-to-day operation of the corporate records management policy within an organisation. May also indicate responsibility for operation of the corporate records management system.
Agency	A generic title for any public sector institution forming part of the national or local executive, judiciary or legislature that creates records and has its own record management system. In legislation the equivalent term may be public office.
Aggregation	Any accumulation of record entities at a level above record object (document, digital object), for example, digital file, series. *Individual records may be aggregated into files and individual files, with their constituent records subsequently aggregated into files (depending on terminology used by the electronic records management system).* See also **File**, and **Record category**.
Application program interface (API)	An application program(ming) interface is the specific method prescribed by a computer operating system or application program so that the application program can make requests of the operating system or another application.
Appraisal	The process of evaluating business activities to determine which records need to be captured and how long the records need to be kept, to meet business needs, the requirements of organisational accountability and community expectations.
Archival authority	The archival agency, archival institution, archival program agency or program responsible for selecting, acquiring and preserving archives, making them available and approving destruction of other records
Archival record	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.
Archival value	The determination in appraisal that records is worthy of permanent preservation by an archival institution.
Archive	The whole body of records of continuing value of an organisation or individual. Sometimes called 'corporate memory'.

Term	Definition
Archives	Materials created or received by a person, family or organisation, public or private, in the conduct of their affairs and preserved because of the enduring value contained in them or as evidence of the functions and responsibilities of their creator, especially those materials maintained using the principles of provenance, original order and collective control; permanent records. Note: This definition differs to the IT sphere where it refers to 'a copy of one or more files or a copy of a database that is saved for future reference or for recovery purposes in case the original data is damaged or lost.' Source: *IBM Dictionary of Computing*, McGraw Hill, New York, 1994, p. 30.
Archives Management	The area of management concerned with maintenance and use of archives / life cycle management.
Archiving	1. The process of creating and transferring computer files or records (or a backup copy of computer files), for long-term storage. 2. Transferring records from a State Agency to the State Archivist.
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 Public Office with respect to the details of the records appraisal process.
Appraisal Management	The area of management that appraises the operational and archival value of records within the agencies.
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.
Audit Trail	A record, or series of records, which allows the processing carried out by a computer or clerical system to be accurately identified, as well as verifying the authenticity of such amendments, including details of the users who created and authorized the amendment(s).
Audit and Quality Management	The area of management that ensures compliance accordance to policies and procedures that is in place by Arkib Negara Malaysia.
Authentication	The process of establishing that the sender of a message is who they claim to be. Source: National Archives of Australia, *Recordkeeping and Online Security Processes: Guidelines for Managing Commonwealth Records Created or Received Using*

Term	Definition
	Authentication and Encryption, 2004.
Backup	1. The process of duplicating information primarily for protection in case the original is lost or destroyed. 2. A copy of the record.
BCS	See **Business classification scheme.**
Business classification scheme (BCS)	1. A conceptual representation of the functions and activities performed by an organisation. The scheme is a taxonomy derived from the analysis of business activity. 2. The basis from which classification tools, such as a functions thesaurus and records classification scheme, are developed. See also **Disposition authority, Records classification tool** and **Taxonomy**.
Business activity	An umbrella term covering all the functions, processes, activities and transactions of an organisation and its employees. Includes public administration as well as commercial business.
Business system	For the purposes of this document, an automated system that creates or manages data about an organisation's activities. Includes applications whose primary purpose is to facilitate transactions between an organisational unit and its customers – for example, an e-commerce system, client relationship management system, purpose-built or customised database, and finance or human resources systems. See also **Electronic document and records management system** and **Electronic records management system** (both are commonly referred to as EDRMS).
Capture	1. The process of lodging a document or digital object into a recordkeeping system and assigning metadata to describe the record and place it in context, thus allowing the appropriate management of the record over time. For certain business activities this functionality may be built into business systems so that the capture of records and associated metadata is concurrent with the creation of records. See also **Registration**. Source: National Archives of Australia, *Digital Recordkeeping: Guidelines for Creating, Managing and Preserving Digital Records,* exposure draft, 2004. Adapted from AS 4390, Part 1, Clause 4.7. 2. The process of fixing the content, structure and context of a record to ensure that it is a reliable and authentic representation of the business activities or transactions in

Term	Definition
	which it was created or transmitted. Once captured within an electronic records management system, users should not be able to alter the content, structure and context of a record.
Certification authority	A body that generates, signs and issues public key certificates that bind subscribers to their public key. Source: National Archives of Australia, *Recordkeeping and Online Security Processes: Guidelines for Managing Commonwealth Records Created or Received Using Authentication and Encryption*, 2004.
Change Management and Communication	A series of activities specifically designed to develop and to enable impacted people to work confidently in their jobs in order to achieve the desired business objective while concurrently undergoing the change process.
Classify	The activity of identifying and arranging records and archives in categories according to logically structured conventions, methods and procedural rules represented in a classification system.
Classification	1. The systematic identification and arrangement of business activities and/or records into categories according to logically structured conventions, methods and procedural rules represented in a classification system. 2. Classification includes determining document or file naming conventions, user permissions and security restrictions on records. See also **Business classification scheme, Records classification scheme** and **Taxonomy**. Source: Adapted from ISO 15489, Part 1, Clause 3.5; AS 4390, Part 1, Clause 4.8.
Collaboration	The Collaboration System is a virtual workplace for a group of identified users working together on an area such as Light discussion, Coordinating works, Collaborate or joint author work, and Maintain team's reference document.
Component	A set of constituent parts that comprises a digital record (such as the multimedia components of a web page). It is necessary to capture metadata about components to enable a record to be managed over time – for example, for migration purposes. Source: Adapted from The National Archives (UK), *Requirements for Electronic Records Management Systems, 3: Reference Document*, 2002, p. 1.
Compound record	A record that comprises multiple individual electronic objects, f*or example, web pages with embedded graphics and style sheets.*
Content	The information conveyed by documentary material.

Term	Definition
Context	The organizational, functional, and operational circumstances in which documentary material is created and/or received and used.
Contextualize	The ability to develop and document the inter-relationship of content between records.
Control	1. The physical and/or intellectual management established over records by documenting information about their physical and logical state, content, provenance and relationships with other records. The systems and processes associated with establishing control include registration, classification, indexing and tracking. See also **Classification** and **Registration**. 2. An IT term for the process of eliminating a record from a system in such a way that the record may still be retrieved if necessary. Also known as 'soft delete'. See also **Destruction**.
Controlled vocabulary	An alphabetical list containing terms or headings that are authorised or controlled so that only one heading or form of heading is allowed to represent a particular concept or name. See also **Thesaurus.** Source: Adapted from J Kennedy and C Schauder, *Records Management: A Guide to Corporate Recordkeeping*, 2nd edition, Longmans, Melbourne, 1988, p. 291.
Conversion	The process of changing records from one medium to another or from one format to another. Conversion involves a change of the format of the record but ensures that the record retains the identical primary information (content). See also **Migration**. Source: Adapted from the ISO 15489, Part 1, Clause 3.7 and Part 2, Clause 4.3.9.2.
Create	To generate a record.
Cryptographic key	The data elements used for the encryption or decryption of electronic messages. They consist of a sequence of symbols that control the operation of a cryptographic transformation, such as encipherment. Source: National Archives of Australia, *Recordkeeping and Online Security Processes: Guidelines for Managing Commonwealth Records Created or Received Using Authentication and Encryption*, 2004.

Term	Definition
Customer Relationship and Consultation Management	An operational process solution that can enhance an organization's ability to see the differences in customer and prospects needs and behaviour based upon the customer's value and priorities. It encompasses marketing and customer service, and focuses on customer experience with the organization.
Data	Groups of characters that represent a specific value or condition. Data provide the building blocks of information.
Database	An organised collection of related data. Databases are usually structured and indexed to improve user access and retrieval of information. Databases may exist in physical or digital format.
Deletion	The process of removing, erasing or obliterating recorded information from a medium outside the disposition process. Deletion within electronic systems generally refers to the removal of the marker (that is, location information) that allows the system to identify where a particular piece of data is stored on the medium. See also **Destruction** and **Disposition**.
Describe	Process whereby records are being identified and classified.
Description	The process of capturing, analyzing, organizing and recording information that serves to identify manage, locate and explain archives and the contexts and records systems that produced them.
Descriptor	A non-hierarchical qualifier (for example, 'Personnel') attached to a security category to limit access to particular records. Descriptors may be informative or advisory but cannot actively control access. Source: Adapted from The National Archives (UK), *Requirements for Electronic Records Management Systems, 3: Reference Document*, 2002, pp. 27–8.
Design specification	A document detailing requirements for functionality, performance and design to be incorporated within a system to be built. The design specification details what is to be built, how it is to be built and how the system will function.
Destruction	1. The process of eliminating or deleting records, beyond any possible reconstruction. 2. In this document, destruction refers to a disposal process whereby digital records, record plan entities and their metadata are permanently removed, erased or obliterated as authorised and approved by a disposition authority schedule. See also **Deletion**. Source: Adapted from ISO 15489, Part 1, Clause 3.8.

Term	Definition
Digital certificate	An electronic document signed by the certification authority which identifies a key holder and the business entity they represent, binds the key holder to a key pair by specifying the public key of that key pair, and should contain any other information required by the certificate profile. Source: National Archives of Australia, *Recordkeeping and Online Security Processes: Guidelines for Managing Commonwealth Records Created or Received Using Authentication and Encryption*, 2004.
Digital file	A set of related digital records held in a tightly bound relationship within the business system and managed as a single object. A type of aggregation of digital records. May also be referred to as a 'container'. See also **Aggregation** and **File**.
Digital object	An object that can be represented by a computer, such as a file type generated by a particular system or software application (for example, a word-processed document, a spreadsheet, an image). A digital record may comprise one or more digital objects. See also **Component**.
Digital signature	A security mechanism included within a digital record that enables the identification of the creator of the digital object and that can also be used to detect and track any changes that have been made to the digital object. Sources: National Archives of Australia, *Digital Recordkeeping: Guidelines for Creating, Managing and Preserving Digital Records*, exposure draft, 2004. Adapted from the Australian Government Information Management Office, *Trusting the Internet: A Small Business Guide to E-security*, 2002, p. 43.
Digital watermark	A complex visible or invisible pattern denoting provenance or ownership information. A watermark may be superimposed on a digital image and can only be removed by use of an algorithm and a secure key. Similar technologies may be applied to digitised sound and moving picture records. Source: Cornwell Management Consultants (for the European Commission's Interchange of Documentation between Administrations Programme), *Model Requirements for the Management of Electronic Records* (MoReq Specification), 2001, p. 70.
Disposition / Disposal	A range of processes associated with implementing retention, destruction or transfer decisions which are documented in disposition or other instruments.

Term	Definition
	Source: ISO 15489, Part 1, Clause 3.9
Disposition action (also Disposal action)	The action noted in a disposition authority indicating the minimum retention period for a record and the event from which the disposal date should be calculated. See also **Disposition trigger** and **Retention period**.
Disposition class (also Disposal class)	A description of the characteristics of a group of records documenting similar activities, together with a disposition action to be applied to the group. The description consists of function and activity terms and scope notes, record description and disposition action. A component of a disposition authority, implemented within a business system as a set of rules made up of a disposition trigger, a retention period and a disposition action, which may be applied to a record plan entity.
Disposal Schedule Validation	Validating the record with the disposal schedule to determine whether or not a record have reached its disposal status.
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.
e-Records	See Electronic Records
Electronic mail (email)	A system that enables users to compose, transmit, receive and manage electronic messages and images across networks and through gateways connecting to other local area networks.
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.
Electronic Records Management	Applying records management principles to electronic records that are located on disks, tapes, or any form of magnetic or optical media.
Extract	A copy of a digital record, from which some material has been removed or permanently masked. An extract is made when the full record cannot be released for access, but part of the record can. Source: Adapted from The National Archives (UK), *Requirements for Electronic Records Management Systems, 3: Reference Document*, 2002, p. 3.
Field	A set of one or more related data elements that represent a category of information within a database.

Term	Definition
	See also **Database**.
File	1. (Noun) An organised unit of documents accumulated during current use and kept together because they deal with the same subject, activity or transaction. 2. (Verb) The action of placing documents in a predetermined location according to a scheme of control. *Note:* For the purposes of this document the records management definition of this term will apply. This differs from the IT definition, which identifies a file as a named collection of information stored on a computer and treated as a single unit. Source: Adapted from J -Ellis (ed.), *Keeping Archives*, 2nd edition, Australian Society of Archivists and Thorpe, Melbourne 1993, p. 470.
File Classification System	A logical and systematic arrangement for classifying records into subject groups or categories based on some definition scheme of natural relationships representing numbers, letters, or key words for identification.
File name	The name given to a group or series of related documents contained in a file folder. Also used to denote the name of an electronic file.
Format	The physical form (such as paper or microfilm) or computer file format in which a record is maintained. See also **Native format**. Source: Adapted from Department of Defense (US), *Design Criteria Standard for Electronic Records Management Software Applications, DoD 5015.2-STD*, 2002, p. 14.
Function	1. The first level of a business classification scheme. Functions represent the major responsibilities that are managed by the organisation to fulfil its goals. Source: Adapted from AS 4390, Part 4, Clause 7.2. 2. The largest unit of business activity in an organisation or jurisdiction.
Graphical user interface (GUI)	A graphical, rather than purely textual, user interface to a computer (for example, windows-style interface).
Guidelines	A set of rules or principles to provide guidance to enable user to carry out certain work processes.
Hybrid file	A set of related digital files and physical files. Both files are held in a tightly bound relationship within the business system and managed as a single object. Records managed within a hybrid file deal with the same subject, activity or transaction.

Term	Definition
	Source: Adapted from The National Archives (UK), *Requirements for Electronic Records Management Systems, 3: Reference Document*, 2002, p. 4.
Hybrid record	1. A set of related digital and physical components that are linked by metadata in a tightly bound relationship and managed as a single record. See also **Physical record** and **Record**. 2. A record consisting of electronic and non-electronic components. *The electronic record and its associated records management metadata is maintained within the electronic records management system together with the records management metadata relating to the non-electronic record.*
Hybrid recordkeeping system	A recordkeeping system containing a combination of paper, electronic or other formats. Source: National Archives of Australia, *Digital Recordkeeping: Guidelines for Creating, Managing and Preserving Digital Records,* exposure draft, 2004.
Identify (Identification)	The process of persistently linking a record or aggregation with a unique identifier. See also **Registration.**
Import	To receive digital records and associated metadata into one system from another, either within the organisation or elsewhere.
Inactive record	Records no longer needed at a particular time for the conduct of current business.
Indexing	The process of establishing access points to facilitate retrieval of records and/or information.
Information and Communication Technology (ICT) Standards Management	Standards as defined by MAMPU.
Inherit	To take on a metadata attribute from a parent entity. Source: Adapted from The National Archives (UK), *Requirements for Electronic Records Management Systems, 3: Reference Document*, 2002, p. 4.
Instance	An occurrence of a digital record in a particular format or at a particular point in time. For example, one instance of a record may be in its native format while another instance is a rendition. Instances may be created as a product of migration or conversion processes.
Integrity	The integrity of a record refers to its being complete and unaltered.

Term	Definition
Internet	The vast network of computer systems that enable worldwide connectivity among users and computers.
Jadual Pemisahan Rekod (Record Retention Schedule)	A document describing the recurring records of a public office, institution or administrative unit, specifying those records to be preserved as having archival value and authorizing on a continuing basis and after the lapse of specified retention periods or the occurrence of specified actions or events, the destruction of the remaining records.
Marker	A metadata profile of a record physically held outside the business system. A marker may denote a physical record (such as a large bound volume or building plan) or an electronic record stored on removable media (such as a CD-ROM or video). A representational link to a relevant record within the electronic records management system to alert users to the existence of a relevant record that is required to be accessible in more than one location. *Note:* A paper file will usually be represented and managed in the business system as a physical file. It is not envisaged that a physical file would contain markers for each document or record placed on a paper file, unless specifically required to do so in order to meet a particular business requirement of the organisation. This may also be referred to as an electronic records management system specific term.
Metadata	Structured or semi-structured information, which enables the creation, management and use of records through time and within and across domains. Source: ISO 23081 – 1: 2006, Clause 4. Structured information that describes and/or allows users to find, manage, control, understand or preserve other information over time. Source: Adapted from A Cunningham, 'Six degrees of separation: Australian metadata initiatives and their relationships with international standards', *Archival Science*, vol. 1, no. 3, 2001, p. 274.
Metadata – Contextualization:	A comprehensive detail of a data which relates one record to another.
Migrate	Act of moving records from one system to another, while maintaining the records' authenticity, integrity, reliability and usability.

Term	Definition
Migration	The act of moving records from one system to another, while maintaining the records' authenticity, integrity, reliability and useability. Migration involves a set of organised tasks designed to periodically transfer digital material from one hardware or software configuration to another, or from one generation of technology to another. Source: Adapted from ISO 15489, Part 1, Clause 3.13 and Part 2, Clause 4.3.9.2.
Native format	The format in which the record was created, or in which the originating application stores records. See also **Conversion**. Source: Adapted from NSW Department of Public Works and Services, *Request for Tender No. ITS2323 for the Supply of Records and Information Management Systems, Part B: Specifications*, 2001, p. 13.
Organize	Setting up a system of directories, which is based on a simple but logical structure which meets the needs of the organization and how it operates?
Permanent record	A record that has sufficient historical or other value to warrant its continued preservation by the Federal Government beyond the time it is needed for administrative, legal, or fiscal purposes.
Physical file	An entry in the record plan for a hardcopy (usually paper) file. The file itself is stored outside the business system but metadata about its location and management is maintained in the system. A physical file may stand on its own within the records classification scheme, or it may form part of a hybrid file of closely related digital and physical objects. See also **File** and **Marker**. Source: Adapted from The National Archives (UK), *Requirements for Electronic Records Management Systems, 3: Reference Document*, 2002, p. 5.
Physical record	A record in hardcopy form, such as a folio, paper file, bound volume, photograph, microfilm, audio recording or moving image recording. See also **Marker, Physical file** and **Record**.
Policy	A formal statement of direction or guidance as to how an organization will carry out its mandate, function or activities, motivated by determined interests or programmes.
Preservation	A broad term covering the range of activities carried out to make sure that records can be retained and remain accessible for as long as they are needed. This includes environmental control, security, storage, handling or

Term	Definition
	processing, migration strategies and disaster preparedness.
Procedures	A process or series of acts especially of a practical or mechanical nature involved in a particular form of work.
Public Archives	Public records which are specified by the Director General as being of permanent and enduring national or historical value or both; and which have been transferred to the National Archives of Malaysia or such other place as the Director General may from time to time direct; and any private records or other material which are specified by the Director General as being of permanent and enduring national or historical value or both acquired for the National Archives of Malaysia by the Director General.
Public Records	Any paper, written or printed book, document or drawing, map or plan, photograph or microfilm, sound-recording or similar device, that has been made or received by any official, officer, board, commission, agency, authority, district, institution or other instrumentality of government, in connection with the transaction of public business and has been retained by an agency as evidence of its activities or because of the information contained therein.
Quality Control	A process to ensure all standards are being followed through Reliability testing and Disposition Testing. See **Reliability Testing** and **Disposition Testing**.
Quality records	Records used to demonstrate conformance to specified requirements and effective operation of quality systems under the AS/NZS ISO 9000 series.
Record (noun)	Information in any format created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business. See also **Hybrid record** and **Physical record**. Source: ISO 15489, Part 1, Clause 3.15.
Record category	A subdivision of the records classification scheme, which may be further subdivided into one or more lower-level record categories. A record category is constituted of metadata which may be inherited from the parent (for example, records category) and passed on to a child (for example, file or aggregation of digital records). The full set of record categories, at all levels, together constitutes the records classification scheme. See also **Records classification scheme**. Source: Adapted from The National Archives (UK), *Requirements for Electronic Records Management Systems, 3: Reference Document*, 2002, p. 1.

Term	Definition
Record type	Definition of a record object which specifies particular management requirements, metadata attributes and forms of behaviour. A default record type is the norm. Specific record types are deviations from the norm, which allow an organisation to meet regulatory requirements (such as privacy or data matching) for particular groups of records. Source: Adapted from The National Archives (UK), *Requirements for Electronic Records Management Systems, 3: Reference Document*, 2002, p. 5.
Records Appraisal	The process of evaluating record based on their current operational, regulatory, legal, fiscal and historical significance, their informational value, arrangement and their relationship to other records.
Records Audit	Conducting a periodic inspection to verify that an operation is in compliance with the records management program.
Records Centre	A low-cost centralized area for housing and servicing inactive or semi-active records whose reference rates does not warrant their retention in a prime office space.
Records classification scheme	A hierarchical classification tool which, when applied to a business system, can facilitate the capture, titling, retrieval, maintenance and disposition of records. A records classification scheme stems from an organisation's business classification scheme.
Records classification tool	A device or method used to assist in classifying, titling, accessing, controlling and retrieving records. May include a records classification scheme, thesaurus, indexing scheme or controlled vocabulary.
Records continuum	The whole extent of a record's existence. Refers to a consistent and coherent regime of management processes from the time of the creation of records (and before creation, in the design of recordkeeping systems), through to the preservation and use of records as archives.
Records Creation and Capture Management	The area of management that encompasses creation of records, the identification and classification of these records and execution of record capture activities.
Records Disposal	After records have reached the end of their retention period in active and/or inactive storage, they may be transferred to an archive for retention or be destroyed.
Records Disposal Management	The area management that handles the Disposal of records. It also conducts reviews on records to ensure that certain criteria are met before the records are disposed. This will be for both the operational and archival records.
Records Disposal Schedule (also Disposal authority)	A formal instrument that defines the retention periods and consequent disposition actions authorised for classes of records described in the authority.

Term	Definition
	See also **Disposition action**, **Disposition class** and **Retention period**. Source: Adapted from AS 4390, Part 1, Clause 4.10. According to the National Archives Act of 2003 (Act 629) "records disposal schedule" means a schedule identifying those records of archival value to be preserved and authorizing the destruction of the remaining records after the lapse of specified retention periods.
Records Lifecycle	An archival concept that describes the lifespan of a record, from its creation or receipt to its final Disposal. The records lifecycle is divided into the following stages or phases: creation/receipt, maintenance and use, retirement, final disposal, and continuing use.
Records Maintenance Management	The area of management whereby the records are organized and maintained, to include the need for records preservation.
Records management	The field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of, and information about, business activities and transactions in the form of records. Source: ISO 15489, Part 1, Clause 3.16.
Records management (Recordkeeping)	The making and maintaining of complete, accurate and reliable evidence of business transactions in the form of recorded information. Recordkeeping includes the creation of records in the course of business activity and the means to ensure the creation of adequate records; the design, establishment and operation of recordkeeping systems; and the management of records used in business (traditionally regarded as the domain of records management) and as archives (traditionally regarded as the domain of archives administration). Source: Adapted from AS 4390, Part 1, Clause 4.19 and Part 3, Foreword.
Records management metadata	Identifies, authenticates and contextualises records and the people, processes and systems that create, manage, maintain and use them, and the policies that govern them. See also **Metadata**. Source: ISO 23081, Part 1, Clause 4.

Term	Definition
Records management system	A framework to capture, maintain and provide access to evidence over time, as required by the jurisdiction in which it is implemented and in accordance with common business practices. Recordkeeping systems include both records practitioners and records users; a set of authorised policies, assigned responsibilities, delegations of authority, procedures and practices; policy statements, procedures manuals, user guidelines and other documents which are used to authorise and promulgate the policies, procedures and practices; the records themselves; specialised information and records systems used to control the records; and software, hardware and other equipment, and stationery. Source: Adapted from AS 4390, Part 3, Clause 6.2.1.
Records Manager	The individual within the organization who is responsible for systematically managing the recorded information generated and received by the organization.
Records Usage and Access Management	The area of management that handles the usage and access of the operational records that includes identifying and monitoring records usage and access.
Recovery	The process of recovering electronic data or documents, without loss, from a corrupted state caused by system or other errors.
Redaction	The process of masking or deleting information in a record.
Register	The process of accepting a record and to document its acceptance.
Registration	The act of giving a record or file a unique identity in a recordkeeping system to provide evidence that it was created or captured. Registration involves recording brief descriptive information about the context of the record and its relation to other records. In the archival context, both aggregations (such as series) and individual record items can be registered. See also **Capture** and **Identify**. Sources: Adapted from ISO 15489, Part 1, Clause 3.18; AS 4390, Part 1, Clause 4.24.
Render	The production of a human-readable representation of a record, usually to a visual display screen or in hardcopy.
Rendition	Instance of a digital record made available in another format or on different medium by a process entirely within the business system control, without loss of content. A rendition should display the same metadata and be managed in a tightly bound relationship with the native format record. Renditions may be required for preservation, access and viewing purposes.

Term	Definition
	See also **Conversion**.
Repository	A place where archived records are preserved and made available for consultation.
Retention period	The length of time after the disposition trigger that a record must be maintained and accessible. At the expiration of the retention period, a record may be subject to a disposition action. See also **Disposition action** and **Disposition trigger**.
Retrieve/Retrieval	1. Process of locating and withdrawing a record from a filing system or records centre. 2. The action of accessing information from stored data on a computer system.
Security	Protection standards and practices imposed a record.
Security category	Hierarchical designation (such as 'Top Secret' or 'Protected') allocated to a user, user role, digital record or other record plan entity to indicate the level of access allowed. The security category reflects the level of protection that must be applied during use, storage, transmission, transfer and disposal of the record. See also **Security controls.** Source: Adapted from Cornwell Management Consultants (for the European Commission Interchange of Documentation between Administrations Programme), *Model Requirements for the Management of Electronic Records* (MoReq Specification), 2001, p. 107.
Security classification system	A set of procedures for identifying and protecting official information, the disclosure of which could have adverse consequences. The security classification system is implemented by assigning markings that show the value of the information and indicate the minimum level of protection it must be afforded. See also **Classification** and **Security category**. Source: Adapted from Attorney-General's Department, *Commonwealth Protective Security Manual*, 2000.
Security controls	A scheme of protective markings which may be allocated to users, digital records and record plan entities to restrict access. May include a hierarchical security category, possibly in conjunction with a non-hierarchical qualifier. See also **Access controls** and **Descriptor**.
Stakeholders	Any individual or group affected by and who are capable of influencing the success of the project.

Term	Definition
Standards	Complex of established norms aiming to make the characteristic of a product, process or service uniformed within or across a sector, country or system.
Standards and Process Management	An area of management whereby standards and processes are continuously developed, reviewed and improved based on current trends and best practices, and Arkib Negara Malaysia's requirements.
Storage / Store	Physical or digital repository for the records.
Structure	The physical or logical form of a documentary material or a set of documentary material.
Structured Environment	Environment in which 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.
System access control	Any mechanism used to prevent access to the business system by unauthorized users. May include the definition of user profiles, or the use of ID and password login.

See also **Access controls** and **Security controls**. |
| **System administrator** | A user role with designated responsibility for configuring, monitoring and managing the business system and its use. May exist at various degrees of seniority with a variety of permissions to undertake system administration functions and some records management processes. |
| **System rules** | Policies internal to system software that may be established and/or configured by a system administrator in order to govern the functionality of a given system and determine the nature of operational processes applied by that system. |
| **Taxonomy** | 1. The classification of entities in an ordered system that indicates natural relationships.
2. The science, laws and principles of classification.

See also **Classification**. |
| **Thesaurus** | 1. In a thesaurus, the meaning of a term is specified and relationships to other terms are shown. A thesaurus should provide sufficient entry points to allow users to navigate from non-preferred terms to preferred terms adopted by the organisation.
2. A records classification tool comprising an alphabetical presentation of a controlled list of terms linked together by semantic, hierarchical, associative or equivalence relationships.

Sources: Adapted from AS 4390, Part 4, Clause 7.3.2.2; AS ISO 15489, Part 2, Clause 4.2.3.2. |

Term	Definition
Tracking	Creating, capturing and maintaining information about the movement and uses of records. Source: ISO 15489, Part 1, Clause 3.19.
Transaction	The smallest unit of business activity. Uses of records are themselves transactions. The third level in a business classification scheme. See also **Activity**, **Business classification scheme** and **Function**. Sources: Adapted from AS 4390, Part 1, Clause 4.27; AS ISO 15489, Part 2, Clause 4.2.2.2.
Transfer	A disposition process, consisting of a confirmed export of digital records and associated metadata, and where applicable aggregations of digital records, followed by their destruction within the exporting business system. Records may be transferred from one organisation to another following administrative change, from an organisation to archival custody, from an organisation to a service provider, from the government to the private sector or from one government to another. Source: Adapted from The National Archives (UK), *Requirements for Electronic Records Management Systems, 3: Reference Document*, 2002, p. 6.
Transfer (custody)	Change of custody, ownership and/or responsibility for records.
Transfer (movement)	Moving records from one location to another.
Unstructured Environment	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 record management 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 record management perspective. Electronic record management solutions tend to be derived from the world of paper based records management.
Usability	A useable record is one, which can be located, retrieved, presented and interpreted.

Term	Definition
Usage	The ability of using and recreating the records via a particular business process.
User access group	Discrete set of named individuals (users known to the business system) that makes up a stable and nameable group. Access to particular records or other file plan entities may be restricted to members of certain user access groups. See also **Access controls**. Source: Adapted from The National Archives (UK), *Requirements for Electronic Records Management Systems, 3: Reference Document*, 2002, p. 28.
User permissions	Privileges allocated to employees determining the extent of access to records and authority to author/originate, add, alter and dispose of records in recordkeeping system.
User profile	A summary of all attributes allocated to a user of the business system. Includes all data known to the system, such as username, ID and password, security and access rights, functional access rights. See also **Access controls**.
User role	An aggregation or standard set of business system functional permissions that may be granted to a predefined subset of system users. Source: Adapted from The National Archives (UK), *Requirements for Electronic Records Management Systems, 3: Reference Document*, 2002, p. 6.
Vital record	Records essential to the continued functioning or reconstitution of an organization during and after an emergency and also those records essential to protecting the rights and interests of that organization and of the individuals directly affected by its activities. Sometimes called essential records. Recommended that there be duplicates located off-site.
Volume	A sub-division of an electronic or non-electronic aggregation. Also referred to as a 'part'. Usually a file part closed off due to size or time period constraints, for example, 'Expense claim forms 2007–2008'. See also **Aggregation**.
Web Environment	Rapidly evolving environment in which, in the earliest stages of web site evolution, organizations find themselves 'publishing' content onto the web (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

Term	Definition
	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).