Australian Government

NATIONAL ARCHIVES OF AUSTRALIA

Recordkeeping Specification

Functional Specifications for Electronic Records Management Systems Software

February 2006

ISBN: 1 920807 34 9

This publication should be cited as: National Archives of Australia, *Functional Specifications for Electronic Records Management Systems Software*, 2006, published at www.naa.gov.au/recordkeeping/er/erms/specifications.html

CONTENTS

EXECUTIVE SUMMARY

The *Functional Specifications for Electronic Records Management Systems Software* provides Australian Government agencies with a set of generic requirements for ensuring adequate recordkeeping functionality within electronic records management systems (ERMS) software.

Agencies are encouraged to make use of the ERMS Specifications when designing or purchasing new, or upgrading existing, ERMS software. The Specifications may also be used when auditing, assessing or reviewing an agency's existing ERMS software.

These generic requirements are not intended to be a complete specification, but rather provide a template of key functional requirements that agencies may incorporate into their tender documentation when preparing to select and purchase new ERMS software. Agencies using the Specifications must assess and amend the functional requirements, and select requirements that best suit their own business and technical requirements and constraints.

1. INTRODUCTION

1.1 Background

In March 2000 the National Archives of Australia launched its *e-permanence* suite of standards, policies and guidelines to assist Australian Government agencies to meet the challenges of digital records management. The centrepiece of the *e-permanence* suite of products is *The DIRKS Manual: A Strategic Approach to Managing Business Information*.[1] DIRKS is a comprehensive methodology intended to help agencies design and implement recordkeeping systems compliant with the *Australian Standard for Records Management,* AS ISO 15489 - 2002.[2]

The DIRKS methodology provides a sound approach for designing recordkeeping systems. However, practical experience indicates a need for detailed advice on evaluating the recordkeeping functionality of software systems, including commercial off-the-shelf software and software designed specifically for agency use.

In 2002, the National Archives surveyed the state of recordkeeping in the Australian government. A high proportion of respondents expressed the need for:

> … guidelines that describe the characteristics of good recordkeeping systems (including generic software specifications).[3]

The survey results also indicated that more practical tools are needed to help agencies undertake DIRKS Steps D to H. This publication, *Functional Specifications for Electronic Records Management Systems Software* (termed hereafter 'the ERMS Specifications' or 'the Specifications') responds to that need.

1.2 Purpose

The ERMS Specifications contains generic requirements for electronic records management systems software. It sets out the recordkeeping functionality that is essential for a system to support business and accountability requirements and meet public expectations. It also presents desirable requirements that may further enhance the recordkeeping functionality of an agency's ERMS software.

The functional requirements set out in the Specifications were developed for Australian Government agencies. This Specification will help agencies:

- build a business case to support the review, design or purchase of ERMS software;
- review the performance of existing ERMS software;

---

1 National Archives of Australia, *The DIRKS Manual: A Strategic Approach to Managing Business Information*, September 2001, published online at www.naa.gov.au/recordkeeping/dirks/dirksman/dirks.html.

2 Standards Australia, *Australian Standard for Records Management,* AS ISO 15489 - 2002.

3 ORIMA Research, *National Archives of Australia: Report on a Survey of the State of Recordkeeping in the Commonwealth Government*, November 2002, p. 66, published online at www.naa.gov.au/recordkeeping/overview/rksurvey_2002.pdf.

- develop requirements for adequate recordkeeping functionality for inclusion in a design specification when building or purchasing ERMS software, or when upgrading existing systems software;
- evaluate the recordkeeping capability of proposed customised or commercial off-the-shelf software intended to manage digital records; or
- undertake a recordkeeping audit or compliance check of agency ERMS software to verify that such systems have adequate recordkeeping functionality.

This specification may be used as a stand-alone product or in conjunction with other National Archives publications, particularly *DIRKS: A Strategic Approach to Managing Business Information* and the *Recordkeeping Metadata Standard for Commonwealth Agencies*, to improve or audit an agency's capacity to manage digital records created or received during the course of its business activities. The Specifications will be of particular use to agencies in the process of identifying recordkeeping functionality for systems, as per Steps D and F of the DIRKS methodology.

1.3 Scope

The ERMS Specifications provides generic requirements for ensuring adequate recordkeeping functionality in ERMS software.

Adequate recordkeeping functionality is intended to reflect the level of functionality that agencies can expect from good quality ERMS software, and exceeds the minimum requirements for recordkeeping functionality as defined in the *Australian Standard for Records Management,* AS ISO 15489.

This publication also contains optional requirements that may, depending on an agency's business needs, be incorporated into its ERMS software to achieve best-practice recordkeeping functionality.

For the purpose of the Specifications, the term 'electronic records management system' encompasses software products designed specifically to manage the creation, use, maintenance and disposal of digital records for the purposes of providing evidence of business activities.[4] These systems maintain appropriate contextual information and metadata, as well as links between records to support their value as evidence.

Use of the term 'systems' within the Specifications is generally intended to refer to computer systems, including software applications, designed for managing digital records. This is distinct from the traditional recordkeeping definition of the term 'systems', which refers to broader recordkeeping systems encompassing a range of elements including organisational policies, procedures and practices, as well as specialised software and hardware and/or paper-based systems required to manage both digital and non-digital records.

[4] Refer to the Glossary for a definition of the term 'ERMS'.

While the Specifications is intended to provide generic functional requirements suitable for all Australian Government agencies, each agency will need to assess and amend the functional requirements to suit its own business and technical requirements and constraints.

The ERMS Specifications provides functional requirements only for systems software specifically designed for the purpose of keeping and managing records. The scope and intended application of the Specifications is explained in more detail in its companion publication, *Guidelines for Implementing the Functional Specifications for Electronic Records Management Systems Software* (ERMS Guidelines).[5]

To determine recordkeeping functionality requirements for other systems that keep digital records (eg business information systems that create and keep digital records in support of their core business functions), please refer to the publication *Functional Specifications for Recordkeeping Functionality in Business Information Systems Software*.[6]

1.4 Audience

The ERMS Specifications is intended for use by all Australian Government agencies. It will be particularly useful to agency staff responsible for managing digital records, primarily staff involved in the development of tender documentation for implementing new records management systems or upgrading existing systems, or staff seeking to audit, assess or review existing ERMS.

The Specifications will also be useful for records and information management software vendors, as the functional requirements it stipulates will inform software developers of the recordkeeping functionality requirements of Australian Government agencies.

1.5 Structure

This publication is arranged in three parts:

- Part 1 introduces the functional requirements, and provides basic guidance on using the Specifications. The ERMS Guidelines contains more detailed information on using the functional requirements.
- Part 2 outlines the core functional requirements for ERMS software. Part 2, Section A describes the core requirements for managing digital records (such as records capture, control, disposal and retrieval). Part 2, Section B describes core requirements for systems management and design (including usability and system administration). These requirements support the records management processes outlined in Section A.

---

5 National Archives of Australia, *Guidelines for Implementing the Functional Specifications for Electronic Records Management Systems Software*, 2006, published online at www.naa.gov.au/recordkeeping/er/erms/guidelines.html.

6 National Archives of Australia, *Functional Specifications for Recordkeeping Functionality in Business Information Systems Software*, forthcoming, to be published online at www.naa.gov.au/recordkeeping/bis/specifications.html.

- Part 3 identifies additional requirements for optional functionality (such as workflow and document management) that may be incorporated in ERMS software or integrated with it. The requirements for optional functionality in Section C expand upon the core requirements in Sections A and B. However, they do not provide a comprehensive specification for the inclusion of such additional functionality. Rather they describe those optional functionality requirements that warrant special consideration to ensure that they do not impair the ability of the ERMS software to perform the core requirements set out in Part 2.

To help users interpret the requirements, this publication includes an extensive glossary.

1.6 Using the Specifications

1.6.1 Key definitions

The requirements outlined in the Specifications use technical terminology drawn from the fields of recordkeeping and information technology. The glossary contains definitions for all key terms and phrases referred to within the functional requirements, detailing how each term should be applied within the context of the Specifications. To correctly understand and apply the Specifications, it is essential that the requirements be read in conjunction with the glossary.

1.6.2 Arrangement of requirements

The requirements in the ERMS Specifications are divided into sections and subsections. Subsections in turn are divided into a number of logical groupings relating to particular aspects of ERMS functionality.

Each functional requirement within the Specifications is presented in a standardised format and has a unique reference number.

1.6.3 Relationships between requirements

Two basic types of functional requirements are contained within the Specifications.

- Non-conditional requirements are stand-alone requirements independent of any other requirement in the Specifications. These requirements are generally phrased: 'The ERMS must/should/may … [description of functional requirement]'.
- Conditional requirements are dependent upon the ERMS supporting one or more specific non-conditional requirements for the conditional requirement to be applicable. These requirements are generally phrased: 'Where the ERMS [supports or does not support a particular feature], it must/should/may … [description of functional requirement]'. Conditional requirements are indented from the rest of the text.

The inter-relation between these two types of requirements is indicated by the applicable obligation levels.

1.6.4 Obligation levels

Each requirement in this document has been allocated an obligation level. The description of each requirement uses the keywords, 'must', 'must not', 'should', 'should not' and 'may' to indicate the obligation levels. These terms reflect established usage in tender documentation.[7]

Mandatory = (M)

This is a compulsory non-conditional requirement for any system intended to keep digital records. 'Mandatory' requirements are essential for the establishment of adequate recordkeeping functionality within all ERMS software. They are identified by the use of the terms 'must' or 'must not'.

Required = (R)

This is a compulsory conditional requirement that applies only when the ERMS supports one or more specific non-conditional requirements. If the ERMS does not support a specified prerequisite non-conditional requirement, the 'Required' requirement will not apply. Required requirements are identified by the use of the prefatory phrase 'Where the ERMS [supports or does not support a particular feature]', and the use of the terms 'must' or 'must not'.

Desirable = (D)

This is an optional requirement for any system intended to keep digital records. These requirements are not considered essential for the establishment of adequate recordkeeping functionality within an ERMS. 'Desirable' requirements generally represent best practice and exceed requirements for adequate recordkeeping functionality. The applicability of desirable requirements must be assessed on a case-by-case basis.

Desirable requirements are identified by the use of the terms 'should', 'should not' or 'may'.

Desirable requirements identified by the use of the terms 'should' or 'should not' are optional but are highly recommended. Agencies should carefully consider their business needs to determine whether such requirements are necessary in their circumstances.

Where a Desirable requirement uses the word 'may', the requirement is considered entirely optional and its implementation is at the discretion of the agency.

Obligation levels often reflect conditional relationships between specific functional requirements. It is not uncommon for a conditional requirement (as defined in Subsection 1.6.3) to stem from an optional non-conditional requirement. If the

---

[7] These terms are further defined in Bradner, S, *Request for Comments 2119: Key words for use in RFCs to indicate requirement levels*, March 1997, published online at www.ietf.org/rfc/rfc2119.txt.

optional non-conditional requirement were not built into the system, the conditional requirement would not apply.

For example, where a Required conditional requirement is dependent upon a Desirable non-conditional requirement, the Required requirement will only come into effect if the optional Desirable requirement has been incorporated into the ERMS software. If the Desirable requirement is not adopted, the Required conditional requirement will not apply.

The ERMS Guidelines contain more information on obligation levels.

1.6.5 Implementing the Specifications

The Specifications contains model requirements that are entirely generic. As such, there has been no consideration of platform-specific or business-related issues. Agencies using these requirements must assess their own organisational context and business needs, and adapt the requirements accordingly.

The ERMS Guidelines provides practical advice to Australian Government agency staff to help them understand and implement the generic requirements set out in the Specifications. The Guidelines explains key terms and concepts, and includes examples of applying the functional requirements in various settings.

1.7 Related products

This publication is part of the *e-permanence* suite of standards, policies and guidelines produced by the National Archives to help agencies manage government information.[8]

Several other *e-permanence* publications can be used in conjunction with the ERMS Specifications to help Australian Government agencies better manage the digital records they create or receive during the course of their business activities. For descriptions of products related to ERMS, see Section 1.6 of the ERMS Guidelines.

1.8 Acknowledgements

The ERMS Specifications are based on similar publications developed locally and internationally. The Specifications has been modified to suit the recordkeeping environment of the Australian Government, in accordance with the requirements of the *Australian Standard for Records Management,* AS ISO 15489 and the National Archives of Australia's *e-permanence* suite of standards, policies and guidelines.

The National Archives of Australia would like to acknowledge the following publications in the development of the ERMS Specifications:

- Commonwealth Department of Family and Community Services, *Request for Tender FACS\02\T296 – Electronic Document Management System (EDMS)*, November 2002
- Cornwell Management Consultants (for the European Commission Interchange of Documentation between Administrations Programme), *Model Requirements for the Management of Electronic Records* (MoReq Specification), March 2001

[8] For information on *e-permanence*, see naa.gov.au/recordkeeping/overview/summary.html.

- The National Archives (United Kingdom), *Requirements for Electronic Records Management Systems*, September 2002
- New South Wales Department of Public Works and Services, *Request for Tender No. ITS 2323 for the Supply of Records and Information Management Systems*, March 2001

References to other relevant publications can be found in the ERMS Guidelines at Appendix 4, 'Further reading'.

The National Archives also notes the contributions of the following staff members:

- Paul Ferridge
- Sonya Sherman
- Melissa Sharkey
- Emma Harris.

2. CORE FUNCTIONAL REQUIREMENTS

A. Records management

A.1 Control

The ERMS must allow folders and records to be organised, so that they can be managed, found and understood.

Business classification scheme

A.1.1	The ERMS should support the representation of a business classification scheme that reflects the business activity of an organisation.	(D)
A.1.2	Where the ERMS supports a business classification scheme, it must be able to track the development and maintenance of the scheme over time.	(R)
A.1.3	Where the ERMS supports a business classification scheme, it must allow centralised management of the scheme by the System Administrator or other authorised user.	(R)
A.1.4	Where the ERMS supports a business classification scheme, it may allow the separate development and use of more than one scheme.	(D)
A.1.5	Where the ERMS supports a business classification scheme, it must allow the definition of levels and the allocation of unique identifiers for business functions, activities and transactions.	(R)
A.1.6	Where the ERMS supports a business classification scheme, it should allow linkages between functions and activities to exist over time.	(R)
A.1.7	Where the ERMS supports a business classification scheme, it may allow the entry of text-based scope notes and other descriptive information attached to functions, activities and transactions.	(D)
A.1.8	Where the ERMS supports a business classification scheme, it may allow the entry of start and end dates for functions, activities and transactions.	(D)
A.1.9	Where the ERMS supports a business classification scheme, it may allow the entry of source citations[9] or mandates attached to functions, activities and transactions.	(D)
A.1.10	Where the ERMS supports a business classification scheme, it may allow the mapping of functions, activities and transactions to organisational structures.	(D)
A.1.11	Where the ERMS supports a business classification scheme, it may allow links to one or more terms in external schemes. For example, the *Australian Government Interactive Functions Thesaurus* (AGIFT) or *Keyword AAA: A Thesaurus of General Terms* (Commonwealth version).[10]	(D)

[9] For example, source citations identified during Step C of a DIRKS project. More information on the DIRKS methodology is available from the DIRKS Manual.

[10] National Archives of Australia, *Australian Governments' Interactive Functions Thesaurus* (AGIFT), 2005, published online at www.naa.gov.au/recordkeeping/gov_online/agift/summary.html. Further information on *Keyword AAA: A Thesaurus of General Terms* (Commonwealth version) is available at www.naa.gov.au/recordkeeping/control/KeyAAA/summary.html.

A.1.12 Where the ERMS supports a business classification scheme, it may be able to import from, or export or link to, other systems where there is a close relationship between functional entities (as defined within the business classification scheme) and the functionality of other systems. (D)

A.1.13 Where the ERMS supports a business classification scheme, it may allow the entry or import of recordkeeping requirements for function/activity sets and for transactions or groups of transactions.[11] (D)

A.1.14 Where the ERMS supports a business classification scheme, it should enable links to records management mechanisms within the ERMS – eg records classification tools, access controls and disposal classes/authorities. (D)

A.1.15 Where the ERMS supports links between a business classification scheme and the records management mechanisms within the ERMS, it must warn a System Administrator when control mechanisms linked to the scheme are updated. (R)

A.1.16 Where the ERMS supports links between a business classification scheme and the records management mechanisms within the ERMS, it must meet the metadata requirements specified for function entities in the *Recordkeeping Metadata Standard for Commonwealth Agencies*.[12] (R)

A.1.17 Where the ERMS supports a business classification scheme, it should be able to export that scheme for use in a receiving system, maintaining all structural links between functions, activities and transactions. (D)

Records classification tools

A.1.18 The ERMS must allow records to be classified in accordance with the organisation's records classification scheme. (M)

A.1.19 The ERMS should allow standard recordkeeping products to be imported and merged with existing records classification tools. Standard recordkeeping products may include *Keyword AAA: A Thesaurus of General Terms* (Commonwealth version) an ISO 2788 or ISO 5964-compliant thesaurus.[13] (D)

A.1.20 The ERMS must support close linkage and interaction between records classification tools and other recordkeeping processes such as capture, access and security, disposal, searching and retrieval, and reporting. (M)

A.1.21 Where the ERMS supports links between the records classification scheme and a business classification scheme, it must ensure those links are maintained or updated when either scheme is amended. (R)

A.1.22 The ERMS must support the definition of a records classification scheme, in order to organise digital folders and records. (M)

A.1.23 The ERMS may be able to copy the definition of an existing records classification scheme from within the ERMS, or import the definition of a records classification scheme from another system. (D)

---

11 Such as those recordkeeping requirements identified during Step C of a DIRKS project. More information on the DIRKS methodology is available from the DIRKS Manual.

12 National Archives of Australia, *Recordkeeping Metadata Standard for Commonwealth Agencies*, published online at www.naa.gov.au/recordkeeping/control/rkms/summary.htm.

13 International Organisation for Standardisation, *Documentation – Guidelines for the Establishment and Development of Monolingual Thesauri*, ISO 2788 – 1986; International Organisation for Standardisation, *Documentation – Guidelines for the Establishment and Development of Multilingual Thesauri*, ISO 5964 – 1985.

A.1.24 The ERMS may support the definition and use of multiple records classification schemes. (D)

A.1.25 The ERMS may allow real-time online data entry to update the definition of a records classification scheme. (D)

A.1.26 The ERMS must ensure that the hierarchical accumulation of terms within the definition of a records classification scheme, results in a unique record category. (M)

A.1.27 The ERMS must allocate a unique identifier to each term defined within a records classification scheme. (M)

A.1.28 The ERMS may allow the entry of start and end dates for each term defined within a records classification scheme. (D)

A.1.29 Where the ERMS supports the entry of start and end dates for classification terms, it must maintain links between previous and subsequent terms. (R)

A.1.30 The ERMS should allow the entry of text-based scope notes and/or descriptions attached to terms defined within a records classification scheme, according to protocols as defined and used in *Keyword AAA: A Thesaurus of General Terms* (Commonwealth version). (D)

A.1.31 The ERMS may allow links between the definition of a records classification scheme and one or more terms in external schemes. For example, the *Australian Governments' Interactive Functions Thesaurus* (AGIFT), *Keyword AAA: A Thesaurus of General Terms* (Commonwealth version) or a business classification scheme. (D)

A.1.32 The ERMS must allow a System Administrator or other authorised user to make global amendments to the definition of a records classification scheme in a single process. (M)

A.1.33 The ERMS should be able to export existing records classification tools (such as a controlled vocabulary dictionary) for use in a receiving system, maintaining all structural links. (D)

A.1.34 The ERMS must be capable of supporting a hierarchical structure for the definition of a records classification scheme to a minimum of two levels. (M)

A.1.35 The ERMS should not limit the number of levels permitted at different points within the definition of a records classification scheme.[14] (M)

A.1.36 The ERMS should allow the use of a controlled vocabulary (such as a thesaurus or indexing scheme) to aid in classifying, titling, accessing and retrieving records. (D)

A.1.37 Where the ERMS supports a controlled vocabulary, it may support the use of multiple controlled vocabularies. (D)

A.1.38 Where the ERMS supports a thesaurus, it should be able to meet the protocols of both functions-based and subject-based thesauruses. (D)

A.1.39 Where the ERMS supports a controlled vocabulary, it should allow terms to be allocated to all defined levels in the record plan. (D)

A.1.40 Where the ERMS supports a controlled vocabulary, it must allow terms to be allocated to an existing entity, and to a new entity upon its creation. (R)

A.1.41 The ERMS must restrict the definition and maintenance of records classification tools to a System Administrator or other authorised user. (M)

A.1.42 The ERMS may support a distributed records classification scheme which can be maintained across a network of digital record repositories. (D)

[14] For example, some parts of the scheme may use three levels, others may use four levels.

Folder management

A.1.43	The ERMS must allow the addition of digital folders to the lowest levels of a defined records classification scheme, in order to organise aggregations of digital records.	(M)
A.1.44	The ERMS must be able to ensure that every folder is allocated to a record category within the records classification scheme.	(M)
A.1.45	The ERMS should not limit the number of folders that can be allocated to a record category or defined within the entire system.	(M)
A.1.46	The ERMS should be able to generate a sequential numeric or alphanumeric reference for a folder as defined by the record plan.	(D)
A.1.47	The ERMS must allow a System Administrator to configure the naming mechanisms for entities within the record plan.	(M)
A.1.48	The ERMS must be able to enforce the use of a records classification tool for naming new entities in the record plan.	(M)
A.1.49	The ERMS must be able to automatically record the date of creation of a folder, as folder metadata.	(M)
A.1.50	The ERMS must allow the separate entry of the date on which a folder was opened, which may precede the folder's date of creation.[15]	(M)
A.1.51	The ERMS must allow a folder or group of folders, and their attached records, to be moved and reclassified within the system by a System Administrator or other authorised user.	(M)
A.1.52	The ERMS must ensure that records attached to a folder remain correctly allocated following reclassification of a folder, so that all structural links remain in place.	(M)
A.1.53	The ERMS must allow the manual or automatic update of all folder and record metadata attributes that are determined by classification, following reclassification of a folder.	(M)
A.1.54	The ERMS must allow a System Administrator or other authorised user to enter (as folder metadata) the reason for the reclassification of a folder or group of folders in one operation.	(M)
A.1.55	The ERMS must retain a history of folder reclassification, including a folder's original location.	(M)
A.1.56	The ERMS must allow a System Administrator or other authorised user to close a folder, ensuring that no new records can be added to that folder (but noting requirement A.1.59).	(M)
A.1.57	The ERMS must automatically record the closing date of a folder and be able to use this metadata to support other records management functions, such as disposal (see requirement A.4.30).	(M)
A.1.58	The ERMS must ensure that closed folders and their contents are still accessible for retrieval and viewing purposes.	(M)
A.1.59	The ERMS must allow a System Administrator or other authorised user to open a previously closed folder for the addition of records, and subsequently close the folder again. This will not automatically update the closure date retained in the folder metadata. The action taken (ie addition of records) must be recorded in the relevant audit trail.	(M)

[15] The date on which a folder was opened reflects the date on which the records within the folder were created. The open date of a folder may therefore predate its creation date if the records contained within the folder were created before the folder itself.

A.1.60 The ERMS must prevent the destruction or deletion of folders, records and associated metadata at all times, except as specified in Section A.4, Disposal. (M)

Control metadata

A.1.61 The ERMS must be able to capture and maintain metadata relating to any business classification scheme or records classification tools it supports, in accordance with the *Recordkeeping Metadata Standard for Commonwealth Agencies* and other relevant standards. (M)

A.1.62 The ERMS must prevent the unauthorised addition or amendment of metadata relating to a business classification scheme or records classification tools. (M)

A.1.63 The ERMS must enable lower levels in a defined records classification scheme hierarchy to inherit metadata from higher levels, at the time of creation. (M)

A.1.64 The ERMS should enable lower levels in a defined records classification scheme hierarchy to inherit metadata retrospectively, following a change to the metadata at a higher level. (D)

A.1.65 The ERMS must support the ability to amend or override inherited metadata by an authorised user. (M)

A.1.66 The ERMS must maintain a record of changes made to the business classification scheme or records classification tools over time. (M)

A.1.67 The ERMS must be able to capture and maintain folder metadata in accordance with the *Recordkeeping Metadata Standard for Commonwealth Agencies* and other relevant standards. (M)

A.1.68 The ERMS must prevent the unauthorised addition or amendment of folder metadata elements. (M)

A.1.69 The ERMS must enable folders to inherit metadata from the records classification scheme at the time of creation of the folders. (M)

A.1.70 The ERMS should enable folders to inherit metadata retrospectively, following a change to the records classification scheme. (D)

A.1.71 The ERMS must support the ability of an authorised user to amend or override metadata inherited by folders. (M)

A.1.72 The ERMS must allow user-defined metadata fields for the entry of descriptive information about the folder. (M)

A.1.73 The ERMS must closely link folder metadata to the functionality it represents. Folder metadata must provide both descriptive information and active support for achieving that functionality automatically. (M)

A.2 Capture

The ERMS must formally capture records regardless of their technical characteristics.

Record capture

A.2.1 The ERMS must ensure that digital objects can be captured, regardless of format and technical characteristics,[16] so that they can be registered and stored as digital records. (M)

A.2.2 Where the ERMS captures a digital object made up of more than one (R)

[16] Data file formats and document types should be specified according to business needs.

component, it must maintain a relationship between all components so that they can be managed as a single record and retain the structural integrity of the record.

A.2.3 The ERMS must allow users to capture, register and store all digital objects in their native format. (M)

A.2.4 The ERMS must be able to capture a digital object even if the generating application is not present. (M)

A.2.5 The ERMS must not limit the number of records that can be allocated to a folder or captured within the entire system. (M)

A.2.6 The ERMS should capture records in a way that is closely aligned or concurrent with the creation of records in the generating application. (D)

A.2.7 The ERMS must be able to capture incoming and outgoing electronic messages and attachments: (M)

- as an automated process; and/or
- as selected and directed by a user.

A.2.8 The ERMS must be able to capture attachments and embedded objects together with electronic messages as either linked records or a single compound record. (M)

A.2.9 The ERMS must allow electronic messages and attachments to be captured from within an electronic messaging system, such as an email client. (M)

A.2.10 The ERMS must allow a user to choose whether to capture an electronic message, such as an email, with attachments as: (M)

- an electronic message only;
- an electronic message with attachments;
- the attachments only;
- any combination of the above.

A.2.11 The ERMS must be able to indicate whether an electronic message in the system has an attachment.[17] (M)

A.2.12 The ERMS must be able to undertake the bulk capture of electronic messages relating to the same transaction. (M)

A.2.13 The ERMS must be able to capture a dynamic document, such as a dynamic web page, as: (M)

- a single compound record;
- an aggregation of linked component records;
- a snapshot – 'frozen' in time;
- a collection of components that can be regenerated upon request; or
- a combination of the above.[18]

A.2.14 The ERMS must support the capture of digital records from a range of records-generating systems.[19] These may include: (M)

- common office packages;
- workflow applications;
- electronic messaging systems;

---

[17] For example, by means of a symbol or special icon.

[18] Strategies for the capture and management of websites as records are provided within *Archiving Web Resources: Guidelines for Keeping Records of Web-based Activity in the Commonwealth Government*, 2001, published online at www.naa.gov.au/recordkeeping/er/web_records/intro.html.

[19] Systems to be supported should be specified according to business needs.

- e-commerce and web transactions;
- imaging and graphic design systems;
- barcode support systems;
- library management systems;
- corporate systems;
- business information systems;
- security administration systems; and
- multimedia applications.

A.2.15 The ERMS must be able to undertake a bulk import of records exported from other records management or document management systems, capturing: (M)

- digital records in their existing format, maintaining their content and structure;
- digital records and their metadata, maintaining the relationships between them; and
- the folder structure to which the records are assigned and associated metadata, maintaining the relationships between them.

A.2.16 The ERMS should support the bulk import of transactional records generated by other systems, using: (D)

- predefined batch file transaction imports;
- edit rules to customise automatic registration of records;
- data integrity validation processes; and
- input queues, including multiple queues for different document types.

A.2.17 The ERMS must be able to perform a direct bulk import of digital records with associated metadata that is presented in accordance with the *Recordkeeping Metadata Standard for Commonwealth Agencies* mapping this to the receiving structures. (M)

A.2.18 The ERMS should be able to perform an indirect import of digital records with no associated metadata, or metadata that is presented in a non-standard format, mapping this to the receiving structures. (D)

A.2.19 The ERMS should be able to import any audit information that may be directly associated with digital records and folders. (D)

A.2.20 The ERMS must provide an application programming interface (API) to support integration with other business information systems, so as to enable the capture and processing of records of transactions in real-time. (M)

Record types

A.2.21 The ERMS must support the definition of different record types as defined by a System Administrator. (M)

A.2.22 The ERMS must be able to manage record types centrally, restricting their use to groups of authorised users. (M)

A.2.23 The ERMS must allow defined record types to behave differently, according to their specified metadata profile and management policy. (M)

A.2.24 The ERMS must support a default record type, which is available to all users with the ability to create records, provided within the ERMS or as defined by System Administrators. (M)

Registration

A.2.25 The ERMS must facilitate the process of registration, whereby a digital object is marked as a formal record and registered into a corporate recordkeeping system. (M)

A.2.26	The ERMS must prevent any unauthorised amendment to the content of a registered digital record, noting requirement A.2.27.	(M)
A.2.27	The ERMS must restrict the ability to amend the content of a registered digital record to the highest level System Administrator, and employ strict controls over the amendment process.[20]	(M)
A.2.28	The ERMS must prevent the destruction or deletion of registered digital records and associated metadata at all times, except as specified in Section A.4, Disposal.	(M)
A.2.29	The ERMS must ensure that each registered record has a viewable registry entry including associated metadata.	(M)
A.2.30	The ERMS must assign a unique identifier to each digital record as it is registered, and store this identifier as metadata with the record.	(M)
A.2.31	The ERMS should allow a System Administrator to configure the format of the unique identifier.	(D)
A.2.32	The ERMS must support the naming of digital records upon registration, allowing the name to differ from a digital object file name or subject line.	(M)
A.2.33	The ERMS should provide features to support the process of naming of digital records. For example: • an automated spell check; and • a warning to be generated if a user attempts to register a record using an identifier that already exists within the ERMS.	(D)
A.2.34	The ERMS must be able to restrict the ability to amend the name of a registered digital record to a System Administrator or other authorised user.	(M)
A.2.35	The ERMS must allow records to be classified in accordance with the organisation's records classification scheme at the time of registration (see A.1, Control).	(M)
A.2.36	The ERMS must ensure that all digital records are assigned to at least one folder upon registration.	(M)
A.2.37	The ERMS should allow a digital record to be assigned to more than one folder.	(D)
A.2.38	The ERMS should warn a user attempting to register a record that is already registered in the same folder, where this can be deduced from captured metadata.	(D)
A.2.39	The ERMS should allow the creation of a new folder 'on the fly', during registration of a record.	(D)
A.2.40	The ERMS should support the classification of records during registration by, for example: • suggesting most recently used terms or folders by default; • suggesting folders which contain known related records; and • displaying sections of the record plan based on record metadata or user profile.	(D)

Record movement

A.2.41	The ERMS must allow the re-assignment of records from one folder to another by a System Administrator or other authorised user.	(M)
A.2.42	The ERMS should provide a controlled copy facility in order to allocate the copied record to a different part of the record plan without changing the contents.	(D)

[20] Amendment of the content of a registered digital record should only take place in exceptional circumstances, such as amending a record in connection with a successful Freedom of Information application.

A.2.43 The ERMS must be able to copy the contents of an existing digital record in order to create a new and separate digital record, ensuring that the original record remains intact. (M)

A.2.44 When a record is retrieved, an ERMS that supports requirement A.2.42 must be able to list and make available all controlled copies of that record. (R)

A.2.45 The ERMS should facilitate the tracking of all copies made of registered digital records, recording information on the movement of copies in the audit log.[21] (D)

A.2.46 The ERMS should facilitate the creation of multiple entries for records in different folders without actual duplication of the digital record. (D)

A.2.47 The ERMS should support a superseded status for records, creating a link to the superseding record. (D)

Record metadata

A.2.48 The ERMS must support the capture and presentation of metadata for digital records as set out in the *Recordkeeping Metadata Standard for Commonwealth Agencies*. (M)

A.2.49 The ERMS must be able to automatically capture metadata acquired directly from an authoring application, an operating system, or generated by the ERMS itself. (M)

A.2.50 The ERMS must be able to capture metadata entered manually by a user during registration. (M)

A.2.51 The ERMS must be able to capture electronic message transmission data and map it to record metadata elements, preventing any amendment. (M)

A.2.52 The ERMS must be able to allow automatically captured metadata to be edited prior to registration of the record, where permitted under A.2.54 and A.2.55.[22] (M)

A.2.53 The ERMS must capture all metadata specified during configuration, and retain it with the digital record in a tightly-bound relationship at all times.[23] (M)

A.2.54 The ERMS must prevent the amendment of selected metadata elements (particularly metadata acquired directly from an authoring application, an operating system, or generated by the ERMS itself) as set out in the *Recordkeeping Metadata Standard for Commonwealth Agencies*. (M)

A.2.55 The ERMS must enable a System Administrator to restrict the ability to amend record metadata, so that: (M)

- only selected metadata elements can be edited by any user during registration;
- selected metadata elements can only be edited by an authorised user during registration; and
- selected metadata elements (as set out in the *Recordkeeping Metadata Standard for Commonwealth Agencies*) can be edited by an authorised user after registration, noting requirement A.2.52.

A.2.56 The ERMS must allow a System Administrator to: (M)

- define customised metadata fields for digital records;
- define the selected metadata element set for particular record types;

---

[21] The audit log should keep details of copies created outside the ERMS, as well as copies created within the ERMS, regardless of the folder(s) in which the copies are retained.

[22] This may be required were automatically generated metadata, such as metadata captured from the 'document properties' information within a document, may be inaccurate or unreliable.

[23] That is, a robust connection inextricably linking the metadata and the digital record to which it relates.

- specify obligation levels for selected metadata elements; and
- reconfigure selected metadata sets as required.

A.2.57 The ERMS must be able to validate the content of specified metadata elements to ensure that they conform to: (M)

- the requirements of the *Recordkeeping Metadata Standard for Commonwealth Agencies*;
- the requirements of other relevant standards (such as those for date and time); and
- any numeric or alphanumeric formats specified at configuration.

A.2.58 The ERMS must be able to store metadata in an easily searchable format, and not solely in audit logs. (M)

A.2.59 The ERMS must be able to store metadata over time, regardless of whether the related record has been archived, deleted or destroyed. (M)

A.2.60 The ERMS must allow manual entry of descriptive information metadata by an authorised user after registration. (M)

A.2.61 The ERMS must capture the date and time of registration as record metadata, and in the audit trail. (M)

A.2.62 The ERMS must enable digital records to inherit metadata from the parent folder within a records classification scheme, at the time of creation. (M)

A.3 Access and security

The ERMS must have the ability to assign rights and restrictions on the use or management of particular records in order to facilitate security.

System access

A.3.1 The ERMS must provide an authentication mechanism which controls access to the system by validating each user (eg user-ID/password login) at the start of a session. (M)

A.3.2 The ERMS should support a mechanism to allow access to the system via integrated network login. (D)

A.3.3 The ERMS must allow a System Administrator to set security parameters for failed login attempts. (M)

A.3.4 The ERMS must restrict the definition and amendment of system access controls to a System Administrator. (M)

A.3.5 The ERMS must be able to link the user-ID to a valid user profile within the system. (M)

A.3.6 The ERMS must allow a System Administrator to define and identify new users, and delete or make inactive existing users. (M)

Access and security controls

A.3.7 The ERMS must support a mechanism for centrally managing access and security controls that may be applied to users, digital records and other entities in the record plan. (M)

A.3.8 The ERMS must restrict the definition and maintenance of access and security controls to a System Administrator. (M)

A.3.9 The ERMS must be able to actively link access and security controls to other records controls employed by the system. (M)

A.3.10 The ERMS must support the definition of discrete user access groups and ad hoc lists of individual users, to control user access to digital records and other entities in the (M)

record plan.

A.3.11 The ERMS must allow a System Administrator to delete or make inactive existing user access groups, effectively barring any access previously allowed by the group(s). (M)

A.3.12 The ERMS should support as a minimum the security categories outlined in the *Commonwealth Protective Security Manual*.[24] (D)

User profiles

A.3.13 The ERMS must require a System Administrator to make users known to the system by means of pre-defined user profiles, supporting valid authentication and the allocation of access and security controls. (M)

A.3.14 The ERMS must allow (but not require) a System Administrator to allocate users to one or more pre-defined user access groups. (M)

A.3.15 The ERMS must require the allocation of a single security category to each user profile, with the default being the lowest category. (M)

A.3.16 The ERMS must restrict the ability to add, amend or delete user profiles to a System Administrator. (M)

A.3.17 The ERMS must allow a System Administrator to define a set of user roles which control the assignment of rights to specific functions or groups of functions. (M)

A.3.18 The ERMS must ensure that all users are allocated one (or more) roles, and allow access only to system functions permitted by the role(s). (M)

A.3.19 The ERMS should allow access and security controls to be allocated to a role and inherited by users. (D)

A.3.20 Where a security category is inherited from a role, the ERMS must allow a different security category to be applied at the individual user level. [25] (R)

Access and security application

A.3.21 The ERMS must allow each user to allocate to records and folders the same access and security controls contained in the user's profile. (M)

A.3.22 The ERMS must prevent users from allocating access and security controls that are **not** contained in the user's profile. (M)

A.3.23 The ERMS should allow the configuration of access and security controls to support complex or unique access and security models. For example: (D)

- the definition of access directions for records and folders, and rules relating to their use; and
- the establishment of layers of access so that a record or folder can have a high-level access ruling (such as 'Open' or 'Closed') and a more specific access or security control (such as 'Restricted: Commercial-in-Confidence').

---

[24] Organisations must determine whether the system is required to store national security classified information. Further information on the Attorney-General's Department publication, *Commonwealth Protective Security Manual*, 2000, is available at www.ag.gov.au/agd/WWW/protectivesecurityhome.nsf/Page/Protective_Security_Manual. *Note:* any system that holds national security-classified information must meet the applicable standards outlined by the Defence Signals Directorate in its *Australian Government Information and Communications Technology Security Manual* (ACSI 33), March 2005, published online at www.dsd.gov.au/library/infosec/acsi33.html.

[25] Consistent rules of precedence must be applied to ensure a single security category is allocated as per requirement A.3.15.

A.3.24 The ERMS must support the allocation of all forms of access and security controls to digital records, folders and other record plan entities, including: (M)
- predefined user access groups (a discrete list of named users);
- one or more individual usernames (an ad hoc list of named users); and
- security categories (only one category may be allocated per entity).

A.3.25 The ERMS must allow any and all combinations of access and security controls to be allocated to digital records, folders and other record plan entities. (M)

A.3.26 The ERMS should support the addition of a descriptor to a digital record or folder, as metadata for informative use.[26] (D)

A.3.27 The ERMS must allow the update and amendment of the access and security controls on digital records, folders and other record plan entities. (M)

A.3.28 The ERMS must restrict access to digital records, folders and other record plan entities that have been allocated a predefined user access group, to those users who are members of that group. (M)

A.3.29 The ERMS must restrict access to digital records, folders and other record plan entities that have been allocated multiple predefined user access groups, to those users who are members of those groups.[27] (M)

A.3.30 The ERMS must limit access to digital records, folders and other record plan entities that have been allocated one or more individual usernames, only to those users so named. (M)

A.3.31 The ERMS must allow all users (unless restricted by user role) access to all digital records, folders and other record plan entities which are not allocated any access or security controls.[28] (M)

A.3.32 The ERMS must restrict access to digital records, folders and other record plan entities, to those users or groups who have been allocated an equivalent or higher security category. (M)

A.3.33 The ERMS must ensure that digital records and folders automatically inherit access and security controls from higher levels of the record plan under which they are created. (M)

A.3.34 The ERMS must allow inherited access and security controls to be overridden by an authorised user, in accordance with the organisation's security model.[29] (M)

A.3.35 The ERMS must be able to automatically upgrade the security category of a digital record or folder, in accordance with the organisation's security model. (M)

A.3.36 The ERMS must require the allocation of a single security category to a digital record, folder or other record plan entity, with the default being the lowest category. (M)

---

[26] For more information on descriptors, see the ERMS Guidelines.

[27] Consistent rules must be applied to ensure the user is (a) a member of any allocated group, or (b) a member of all allocated groups – according to business requirements.

[28] Apart from the default lowest security category as per requirement A.3.15.

[29] The security model must specify whether a digital record or folder is permitted a lower or higher security category than the folder or record category in which it is contained. For more information, see the ERMS Guidelines.

A.3.37 The ERMS must restrict access to digital records, folders and other record plan entities which have been allocated one or more forms of access and security controls, only to those users who have been allocated all equivalent controls – and prevent access by users who have been allocated some, but not all, equivalent controls.[30] (M)

A.3.38 The ERMS should support several options for viewing records that are allocated access and security controls, including: (D)

- users without appropriate permissions are restricted from viewing either the metadata or the record – this includes retrieval through searching, reporting and navigating;
- users without appropriate permissions may view the metadata, but access to the record is restricted; and
- users without appropriate permissions may view the metadata and the record; however, edit access is denied.

Access and security metadata

A.3.39 The ERMS must support the progressive addition of metadata to digital records and folders to support access and security as set out in the *Recordkeeping Metadata Standard for Commonwealth Agencies*. (M)

A.3.40 The ERMS should be able to retain the details and date of amendments to access and security controls, as historical metadata for a user profile, digital record, folder or other record plan entity. (D)

A.3.41 The ERMS must support the progressive addition of metadata to digital records and folders to support privacy, freedom of information and archives legislation, [31] including: (M)

- information about the release of digital records and folders, which may be used to retrieve details from another system;
- disclosability and exemption indicators; and
- full details of record creation, modification and preservation to assist in determining the age of long-term records,

as set out in the *Recordkeeping Metadata Standard for Commonwealth Agencies*.

Extraction

A.3.42 The ERMS must allow the creation of an extract from a digital record, whereby sensitive information is removed or hidden from view[32] in the extract, while the originating record remains intact. (M)

A.3.43 The ERMS must provide solutions for expunging sensitive information from all record formats it can capture, including audio and video. (M)

A.3.44 The ERMS must note the creation of an extract in the metadata of the originating digital record, including date, time, creator and reason for creation of the extract. (M)

A.3.45 The ERMS must be able to copy metadata attributes from the originating digital record to an extract – allowing selected elements to be amended as necessary.[33] (M)

---

30 For more information, see the ERMS Guidelines.

31 The *Privacy Act 1988*, *Freedom of Information Act 1982* and *Archives Act 1983*.

32 For example, individual pages can be removed from a multi-page record, and opaque rectangles can be used to obscure selected words.

33 For example, an extract may have a different security category from the originating record.

A.3.46 The ERMS should be able to register an extract as a record in its own right, noting requirements A.3.44 and A.3.45. (D)

A.3.47 The ERMS should create a navigable link between an extract and the digital record from which it was taken. Such a link should preserve the relationship between the extract and the digital record without compromising the access and security controls applicable to the record. (D)

A.3.48 Where the ERMS allows the creation of a navigable link between an extract and the digital record from which it was taken, the link must not compromise the access and security controls applicable to the record. (R)

Audit trail

A.3.49 The ERMS should monitor access to its facilities and all data held within those facilities; in an audit log, the ERMS should maintain: (D)

- a list of users who have accessed the system, including date and time of access and length of session;
- failed login attempts;
- failed attempts to view digital records;
- attempts to access restricted areas of the record plan; and
- attempts to access system functions restricted to the System Administrator.

A.3.50 The ERMS must be able to maintain a complete record of all events performed within the system as an audit trail, including: (M)

- the action carried out;
- the object of the action;
- the user undertaking the action; and
- the date and time of the event.

A.3.51 The ERMS may initiate the audit trail automatically as a result of system parameters. (D)

A.3.52 The ERMS must ensure that actions undertaken by a System Administrator are captured in the audit trail, including configuration and reconfiguration of the audit trail itself. (M)

A.3.53 The ERMS must be able to record the details of all activities performed on digital records, folders and groups of folders, extracts and all associated metadata. (M)

A.3.54 The ERMS must protect the audit trail against modification by any user, including a System Administrator. (M)

A.3.55 The ERMS must manage audit trails as records and retain them according to the *Administrative Functions Disposal Authority*.[34] (M)

A.3.56 The ERMS must ensure that audit trail data can be made available for inspection upon request. (M)

A.3.57 The ERMS should allow audit trail data to be easily exported without affecting the audit trail stored within the ERMS. (D)

---

[34] National Archives of Australia, *Administrative Functions Disposal Authority*, 2000, published online at www.naa.gov.au/recordkeeping/disposal/authorities/GDA/AFDA/summary.html.

A.3.58 The ERMS must be able to automatically record information in the audit trail about the following events: (M)

- creation of a new user or group;
- date and time of registration of all records;
- changes to access and security controls affecting a record, folder or user;
- relocation of records to another folder, identifying both origin and destination;
- relocation of a folder to a different part of the record plan, identifying both origin and destination;
- date and time of a change made to metadata associated with folders or records;
- all disposal review decisions made by a System Administrator;
- reapplication of a disposal authority to an entity, identifying both previous and subsequent authorities;
- placing or removing of a disposal freeze on a record or folder; and
- a separate log of all deletion or destruction actions carried out by any user.

A.4 Disposal

The ERMS must be able to control the retention and disposal of records held by the system, in accordance with disposal authorisation.

Disposal authorities

A.4.1 The ERMS must support the controlled disposal of records legally authorised for disposal, either in accordance with approved disposal authorities issued by the National Archives or in accordance with a specific legislative requirement for the disposal of particular records.[35] (M)

A.4.2 The ERMS must enable the definition of rules for disposal classes, which can be applied to selected digital records and record plan entities where supported. (M)

A.4.3 The ERMS must support the definition and application of the following disposal actions: (M)

- review;
- export;
- transfer;[36] and
- destruction.

A.4.4 The ERMS must be able to import and export a set of disposal classes in a standard format defined by the National Archives.[37] (M)

A.4.5 The ERMS must allow a unique identifier to be assigned to each disposal class and, where applicable, must allow the disposal class to be associated with the appropriate disposal authority.[38] (M)

---

35 Where a disposal action is positively required under any Commonwealth law, the approval of the National Archives for disposal is not required.

36 Transfer consists of confirmed export followed by destruction, once the success of the transfer process has been confirmed.

37 A structured set of disposal classes issued by the National Archives is known as a 'disposal authority'.

A.4.6 The ERMS must be able to maintain a history of all changes to disposal classes, including date of change and reason for change. (M)

A.4.7 The ERMS must restrict the ability to create, edit and delete disposal classes and disposal authorities to the System Administrator or other authorised user. (M)

A.4.8 Where the ERMS supports links between a business classification scheme and disposal functions, it may enable terms from the scheme to form the basis of disposal classes. (D)

A.4.9 Where the ERMS supports links between records classification tools and disposal functions, it may enable controlled terms from a tool to form the basis of disposal classes. (D)

A.4.10 Where the ERMS supports links between disposal functions and other records management mechanisms within the ERMS, it must warn a System Administrator when control mechanisms linked to disposal classes are updated, and protect disposal classes from amendment until revisions are complete. (R)

A.4.11 The ERMS must be able to manage a many-to-one relationship where multiple disposal classes may be linked to a single record plan entity. (M)

A.4.12 The ERMS must allow retention periods to be defined from one day to an indefinite length of time. (M)

A.4.13 The ERMS must ensure each class consists of: (M)

- a disposal trigger, to initiate the retention period;
- a retention period, to establish how long the record must be maintained; and
- a disposal action, to prescribe the fate of the record.

A.4.14 The ERMS must enable flexibility in the definition of disposal classes to allow the System Administrator to assign non-standard retention periods and disposal actions.[39] (M)

A.4.15 The ERMS must ensure that amendments to a disposal class take immediate effect on all objects to which that class has been applied. (M)

A.4.16 Where the ERMS supports disposal classes, it should: (D)

- support the definition of multiple disposal authorities; or
- allow disposal authorities to be merged during import.

Disposal application

A.4.17 The ERMS must allow disposal classes to be systematically applied to digital records, folders and other record plan entities where supported. (M)

A.4.18 The ERMS should be able to apply sentencing on creation by automatically applying a disposal class to a new digital record or folder, based upon a set of pre-defined instructions.[40] (D)

A.4.19 The ERMS may support automatic sentencing of a digital record or folder based (D)

---

[38] Disposal classes issued by the National Archives post-July 1999 will have a unique identifier or class number. Where the National Archives has not issued a unique identifier for a disposal class, it will be necessary to identify the disposal class in relation to the disposal authority to which it relates. For example, 'RDA 1234/1.1'.

[39] For example, 'destroy when superseded' or 'disposal not authorised'.

[40] For example, based on links to a classification scheme or a particular record type.

upon its contents, specified metadata elements, or a combination of both.

A.4.20 The ERMS must allow a disposal class to be applied at any level in the record plan, and inherited by descendant objects as they are created. (M)

A.4.21 The ERMS must enable the manual update or retrospective inheritance of disposal classes when a new disposal class is applied at a higher level of the record plan.[41] (M)

A.4.22 The ERMS must allow an authorised user to apply a disposal class that overrides an inherited disposal class. (M)

A.4.23 The ERMS must record all disposal actions in an audit trail. (M)

A.4.24 The ERMS must automatically track the initiation and progress of retention periods, in order to determine disposal dates for digital records or folders. (M)

A.4.25 The ERMS must allow an authorised user to apply a different disposal class to an object at any time. (M)

A.4.26 The ERMS must restrict the ability to apply and reapply disposal classes to the System Administrator or other authorised user. (M)

A.4.27 The ERMS must support a disposal process consisting of: (M)

- automatic identification of digital records and folders for which the retention period has elapsed;
- notification of a System Administrator or other authorised user;
- reapplication of a disposal class if required;[42] and
- execution of the relevant disposal actions after confirmation by a System Administrator or other authorised user.

A.4.28 The ERMS must restrict the operation of the disposal process to a System Administrator or other authorised user. (M)

A.4.29 Where the ERMS supports folders, it must ensure that any disposal action applied at folder level is carried out on the complete folder contents. (R)

A.4.30 The ERMS must support a range of internal disposal triggers based on active metadata. For example: (M)

- date of record registration;
- date of last retrieval of a record;
- opening or closing date of a folder; and
- date of last review of a folder or record.

A.4.31 The ERMS must ensure that a retention period is calculated in real time and cannot be artificially advanced. (M)

A.4.32 The ERMS must support external disposal triggers based on notification of a defined event as entered by a user. (M)

A.4.33 The ERMS must automatically seek confirmation from a System Administrator or other authorised user before implementing any disposal action. (M)

A.4.34 The ERMS must allow a disposal freeze to be placed on a digital record, folder or other record plan entity, in order to prevent any disposal action from taking place for the duration of the freeze.[43] (M)

---

41 A new class might be the result of reclassification or of directly applying a different disposal class to an object.

42 Reapplication of a disposal class must take immediate effect within the disposal process.

A.4.35 The ERMS must prevent the deletion of any object subject to a disposal freeze.[44] (M)

A.4.36 The ERMS must restrict the ability to remove a disposal freeze to a System Administrator or other authorised user. (M)

A.4.37 The ERMS may support an interface with a workflow engine to facilitate the disposal process.[45] (D)

A.4.38 The ERMS must be able to identify any conflict between disposal actions and either: (M)

- automatically apply the correct disposal action according to precedence defined by the organisation; or
- notify the System Administrator or other authorised user and request remedial action.

A.4.39 The ERMS must be able to notify the System Administrator on a regular basis of all disposal actions due to occur in a specified period of time. (M)

Review

A.4.40 The ERMS must make all metadata relating to a digital record or folder under review available to the reviewer. (M)

A.4.41 The ERMS must make the entire contents of a digital record or folder under review available to the reviewer, subject to applicable access restrictions. (M)

A.4.42 The ERMS must make the applicable disposal class details available to the reviewer either by searching or navigation. (M)

A.4.43 The ERMS should automatically record the date of last review as active metadata, and allow the reviewer to add the reasons for the review decision as descriptive metadata. (D)

A.4.44 When a review disposal action is triggered, the ERMS must allow the System Administrator to reapply a disposal class which could: (M)

- mark digital records and folders for further retention and later review;
- mark digital records and folders for immediate export, transfer, preservation treatment (through a technique such as migration) or destruction; or
- mark digital records and folders for further retention and later export, transfer, preservation treatment (through a technique such as migration) or destruction.

Export and transfer

A.4.45 The ERMS must be able to export digital records, folders or other record plan entities, and all associated metadata to: (M)

- another system within the organisation;
- a system in a different organisation; or
- the National Archives for the long-term preservation of digital records appraised as having archival value.

---

[43] A disposal freeze may be placed on records identified as being subject to a pending or ongoing Freedom of Information application or legal discovery process, as well as those records subject to a formal National Archives' disposal freeze.

[44] Under other circumstances, deletion may be carried out by a System Administrator or authorised user. See requirement A.4.27.

[45] See workflow requirements at Section C.3.

A.4.46 The ERMS must ensure that any export action is able to include: (M)
- all digital records and folders that qualify for export under a disposal class;
- all metadata associated with exported digital records, folders and other record plan entities; and
- all audit trail data associated with exported digital objects.

A.4.47 The ERMS must be able to export groups of digital records or folders in one sequence of operations such that: (M)
- the content and structure of digital records and folders are not degraded or corrupted;
- all components of a digital record are exported as one unit;
- associations are retained between exported objects and their metadata; and
- relationships are maintained between exported objects so that their structural links can be re-built in the receiving system.

A.4.48 The ERMS must be able to export all the types of records it can capture, regardless of format or the presence of the generating application. (M)

A.4.49 The ERMS must be able to export digital records in their native format (or the current format to which they have been migrated). (M)

A.4.50 The ERMS may be able to export digital records that have been converted into open, fully documented formats consistent with the National Archives' archival data formats.[46] (D)

A.4.51 The ERMS must allow digital objects to be exported more than once. (M)

A.4.52 The ERMS must support a two-stage transfer process, consisting of: (M)
- export of all digital records and folders that qualify for transfer under a disposal class; and
- destruction of the exported digital records and folders following confirmation of successful export.[47]

Destruction

A.4.53 The ERMS must ensure that destruction results in the complete obliteration or inaccessibility of all objects as authorised, that they cannot be restored through operating system features or specialist data recovery techniques.[48] (M)

A.4.54 The ERMS must seek confirmation of destruction from a System Administrator or other authorised user as part of the disposal process. (M)

---

[46] The records may be converted into open formats directly during capture or export, or indirectly through integration with other software. Currently the National Archives will accept transfers of digital records of archival value in their current data formats, as per records exported under requirements A.4.48 and A.4.49. However, the National Archives digital preservation strategy is founded on converting transferred archival value digital records into open, fully documented formats suitable for long-term preservation. Agencies may find it beneficial to incorporate the ability to export digital records in the preferred archival data formats, within their ERMS software. Information about the National Archives' archival data formats is available from www.naa.gov.au/recordkeeping/preservation/digital/xml_data_formats.html. Further information about the digital preservation strategy is available from www.naa.gov.au/recordkeeping/preservation/digital/summary.html.

[47] Digital records and folders must remain intact until confirmation is received from the Systems Administrator or an authorised user.

[48] Excluding controlled disaster recovery or business continuity procedures.

A.4.55	The ERMS must prevent the destruction of digital records or folders until confirmation is received, and allow the process to be cancelled if confirmation is not received.	(M)
A.4.56	The ERMS must distinguish between an ad hoc delete function and the destruction function within the disposal process, so that each can be allocated individually to authorised users.[49]	(M)
A.4.57	The ERMS must have the ability to ensure that when a digital record is authorised for destruction, all alternative renditions of that record are also destroyed.	(M)
A.4.58	The ERMS must allow a System Administrator to turn off the functionality outlined in A.4.57 if required.[50]	(M)
A.4.59	The ERMS must prevent the delete function being used within the disposal process, so that immediate destruction can only be achieved through the allocation of a disposal class.	(M)

Disposal metadata

A.4.60	The ERMS must support the progressive addition of metadata to digital records and folders to support disposal as set out in the *Recordkeeping Metadata Standard for Commonwealth Agencies.*	(M)
A.4.61	The ERMS must be able to export metadata in an XML format, as specified by the *Recordkeeping Metadata Standard for Commonwealth Agencies.*	(M)
A.4.62	The ERMS should allow users to add any metadata elements required for the archival management of digital records selected for transfer.	(D)
A.4.63	The ERMS must actively link disposal metadata to the functionality it represents, so that it can be used to trigger automated processes.	(M)
A.4.64	The ERMS should support free text fields for user-definable notes.[51]	(D)
A.4.65	The ERMS may support the entry of management metadata for disposal classes and disposal authorities, including: • a scheduled review date; • date and details of revision; and • date and details when superseded.	(D)
A.4.66	The ERMS should be able to maintain a history of the disposal classes that have been applied to a particular object, in the metadata of that object.	(D)
A.4.67	The ERMS must be able to detect any metadata changes that affect the retention period of an object, and calculate a new disposal date according to the disposal class.	(M)
A.4.68	The ERMS must be able to restrict the amendment of metadata that affects the retention period of an object to a System Administrator or other authorised user.	(M)
A.4.69	The ERMS must be able to retain metadata for digital records and folders that have been transferred or destroyed.	(M)
A.4.70	The ERMS should allow a System Administrator to specify a subset of metadata[52] to be retained for digital records and folders that have been transferred, destroyed or moved offline.	(D)

---

[49] For information on deletion requirements, refer to Section B.3, System Administration.

[50] For example, if a disposal authority does not cover all renditions, or if an agency has reason to keep a particular rendition.

[51] For example, to link a disposal decision to retention requirements found in legislation.

A.4.71 The ERMS may allow a System Administrator to archive[53] the metadata retained for digital records and folders that have been transferred or destroyed. (D)

A.4.72 The ERMS must be able to record the date and details of all disposal actions as folder and/or record metadata. (M)

A.5 Searching and retrieval

The ERMS must be able to retrieve digital records and folders by a variety of search methods, and render the results on-screen.

Search

A.5.1 The ERMS must support the input of user-defined parameters for the purpose of locating, accessing, retrieving and viewing records, folders and other record plan entities, and associated metadata. (M)

A.5.2 The ERMS must provide search facilities to meet the needs of a range of users, from casual to sophisticated. (M)

A.5.3 The ERMS should provide an optional search and display interface via a web browser platform. (D)

A.5.4 The ERMS must support browsing of the record plan, to folders and their contents; and the direct selection, retrieval and display of digital records and folders in this manner. (M)

A.5.5 The ERMS must be able to withhold all or part of a search result, according to access and security controls as specified in A.3, Access and security. (M)

A.5.6 The ERMS must be able to search all metadata elements, as set out in the *Recordkeeping Metadata Standard for Commonwealth Agencies*. (M)

A.5.7 The ERMS should be able to search the full-text content of digital records. (D)

A.5.8 The ERMS must support the construction of searches by combining multiple terms from multiple sources. (M)

A.5.9 The ERMS must allow the qualification of search terms, for example by specifying a metadata element or record content as the source. (M)

A.5.10 Where the ERMS supports a controlled vocabulary, it must be able to search on terms from the controlled vocabulary. (R)

A.5.11 The ERMS must support the configuration of default search options for end users. (M)

A.5.12 The ERMS must support the definition, saving and re-use of searches by end users. (M)

A.5.13 The ERMS may allow saved search results to be exported from the system in a common data format (eg a plain text, comma separated value, or tab delimited computer file type). (D)

A.5.14 The ERMS should support the use of search logic such as Boolean operators, partial matches, and wildcard characters. (D)

---

52 As set out in the *Recordkeeping Metadata Standard for Commonwealth Agencies*.

53 That is, take a copy which is outside the control of the ERMS.

A.5.15 The ERMS may support the use of advanced search features such as: (D)
- probabilistic retrieval;
- relevancy feedback;
- pattern matching;
- forward, backward and embedded expansion of wildcards;
- relational operators; and
- phonetic searching.

A.5.16 The ERMS must allow searching within and across folders and record categories. (M)

A.5.17 The ERMS should allow users to specify searches based on: (D)
- named time intervals;
- calendar dates; and
- number of days.

A.5.18 The ERMS should allow users to refine and narrow searches using the results of a previous search. (D)

A.5.19 The ERMS must present search results as a list of digital records and folders meeting the search criteria. (M)

A.5.20 The ERMS must notify a user if the search results in a null set. (M)

A.5.21 The ERMS should support the configuration of display formats for search results, allowing a user to specify: (D)
- the order in which the search results are presented;
- the number of 'hits' to be displayed on the screen per view from the search;
- the maximum number of 'hits' to be returned for a search; and
- which metadata fields are displayed in search results.

Retrieval

A.5.22 The ERMS must be able to retrieve digital records and folders by all implemented naming principles. (M)

A.5.23 The ERMS must be able to retrieve digital records and folders directly by their associated unique identifiers. (M)

A.5.24 The ERMS must be able to retrieve a complete folder and all its digital records and contextual metadata, and list all and only those records in the context of that folder as a discrete group and in a single retrieval process.[54] (M)

A.5.25 The ERMS must be able to retrieve and list a set of digital records, taken from many different folders, where the record metadata or content meets the search criteria. (M)

A.5.26 The ERMS must support the simultaneous retrieval of digital records, folders and metadata by multiple users. (M)

A.5.27 The ERMS should allow an electronic message retrieved by the system to be copied to a compatible application and transmitted in the usual manner. (D)

---

[54] The process may consist of a number of operations, but must not require the user to re-enter data already retrieved.

Display

A.5.28	The ERMS must be able to display the content of all the types of digital records which it is able to capture, in a manner that presents all components of the digital record together as a unit.	(M)
A.5.29	The ERMS must display the content of all the types of digital records it can capture, in a manner that renders their original visual presentation and layout, without needing to load the generating application.	(M)
A.5.30	The ERMS must allow digital records and folders retrieved and listed as the result of a search, to be selected then opened by a single keystroke or mouse-click from the search screen.	(M)
A.5.31	The ERMS must be able to display all available metadata associated with a digital record or folder upon request.	(M)
A.5.32	The ERMS must support integrated searching across metadata and record content, and a user interface which appears the same for all levels of the record plan.	(R)
A.5.33	The ERMS should support the presentation or publication of digital records, folders and associated metadata to a destination outside the system.[55]	(D)

Printing

A.5.34	The ERMS must be able to print all the types of digital records it can capture, without the use of 'screen dumps'.[56]	(M)
A.5.35	The ERMS must be able to print the list of digital records and folders returned by a search query.	(M)
A.5.36	The ERMS must enable the printing of metadata associated with digital records and folders.	(M)
A.5.37	The ERMS should allow all the digital records in a folder to be printed in one operation.[57]	(D)
A.5.38	The ERMS must include features for the suitable output of digital records that cannot be printed.[58]	(M)

A.6 Metadata

The ERMS must support the use of metadata to describe digital records and to enable automated records management processes.

Metadata configuration

A.6.1	The ERMS must support the range of metadata elements detailed in the *Recordkeeping Metadata Standard for Commonwealth Agencies* and any other elements required to support the organisation's business.	(M)
A.6.2	The ERMS must be able to draw together all elements of metadata to create a metadata profile for a digital record, folder or other record plan entity where supported.	(M)

55 For example, publication on a website or intranet.

56 Where the record format itself is printable.

57 Those that are printable.

58 For example, audio or video records.

A.6.3	The ERMS must be able to manage the metadata profile as a single entity, noting requirement A.6.15.	(M)
A.6.4	The ERMS must place no practical limitation on the number of metadata elements allowed for each object in the system.	(M)
A.6.5	The ERMS must allow the System Administrator to specify which metadata elements are to be entered and maintained by keyboard entry or by pull-down list.	(M)
A.6.6	The ERMS should support several formats or combinations of formats for metadata elements, including: • alphabetic; • alphanumeric; • numeric; • date/time; and • logical (ie YES/NO or TRUE/FALSE)	(D)
A.6.7	The ERMS must allow a System Administrator to define the source of data for each metadata element.	(M)
A.6.8	The ERMS must have the ability to use the contents of a metadata element to determine a functional process, where the element can be related to the functional behaviour of the ERMS.	(M)
A.6.9	The ERMS should allow metadata values to be obtained from lookup tables or calls to other software applications.	(D)
A.6.10	The ERMS must support the following mechanisms for validating the contents of metadata elements: [59] • format of the element contents; • range of values; • validation against a pre-defined list of values; and • valid classification scheme reference.	(M)
A.6.11	The ERMS may support validation of metadata elements using checksum algorithms.[60]	(D)
A.6.12	The ERMS must, where required, support validation of metadata using calls to another application.	(M)
A.6.13	The ERMS must support persistent default values for selected metadata elements, which are user-definable.	(M)
A.6.14	The ERMS should be able to recognise the value of a metadata element stored in number or date format, for purposes of searching.	(D)
A.6.15	The ERMS must be able to manage a metadata profile independently over time – maintaining links to the record and adding process metadata about records management activities.	(M)

[59] Noting also requirement A.2.57.

[60] For example, an application programming interface may be provided to support this functionality.

A.7 Compliance

The ERMS must meet relevant local, national and international requirements for recordkeeping and records management.

Legislation

A.7.1 The ERMS must support compliance with the recordkeeping, evidential, privacy and access provisions of all relevant federal legislation[61] and regulations, including the: (M)

- *Archives Act 1983*;
- *Commonwealth Authorities and Companies Act 1997*;
- *Electronic Transactions Act 1999*;
- *Evidence Act 1995*;
- *Financial Management and Accountability Act 1997*;
- *Freedom of Information Act 1982*;
- *Privacy Act 1988*; and
- *Public Service Act 1999*.

Standards

A.7.2 The ERMS should support compliance with all applicable Australian and International standards,[62] including where relevant: (D)

- *AGLS Metadata Element Set*, AS 5044 – 2002;
- *Australian Standard for Records Management,* AS ISO 15489 – 2002
- *Commonwealth Protective Security Manual*;
- *Documentation – Guidelines for the Establishment and Development of Monolingual Thesauri,* ISO 2788 – 1986;
- *Documentation – Guidelines for the Establishment and Development of Multilingual Thesauri,* ISO 5964 – 1985;
- *Data Elements and Interchange Formats – Information Interchange – Representation of Dates and Times,* AS ISO 8601 – 2003;
- *Quality Management Systems*, AS ISO 9001 – 2000
- *Information Security Management,* AS ISO 17799 – 2001; and
- *Recordkeeping Metadata Standard for Commonwealth Agencies*.

---

[61] Common legislative requirements have been incorporated into the core requirements where possible; however, it is possible that additional legislative requirements particular to the agency may also need to be accommodated. The agency is responsible for ensuring all legislative requirements are addressed and for establishing measures by which the extent of compliance with this requirement can be measured. For more information, refer to the ERMS Guidelines.

[62] Common applicable standards have been incorporated into the core requirements where possible; however, it is possible that additional standards may need to be accommodated to meet the particular business needs of the agency. The agency is responsible for ensuring all applicable standards are addressed within the requirements and for establishing measures by which the extent of compliance with this requirement can be measured. For more information, refer to the ERMS Guidelines.

Guidelines

A.7.3 The ERMS should support best practice in accordance with all applicable guidelines,[63] including where relevant: (D)

- *Archiving Web Resources: Guidelines for Keeping Records of Web-based Activity in the Commonwealth Government*;
- *Australian Government Information and Communications Technology Security Manual* (ACSI 33);[64]
- *Australian Governments' Interactive Functions Thesaurus* (AGIFT);
- *Commonwealth Procurement Guidelines*;[65]
- *Developing a Functions Thesaurus for Commonwealth Agencies;*[66]
- *Disaster Preparedness Manual for Commonwealth Agencies*;[67]
- *Digital Recordkeeping: Guidelines for Creating, Managing and Preserving Digital Records*;[68]
- *Information Privacy Principles under the Privacy Act 1988*;[69]
- *Recordkeeping and Online Security Processes: Guidelines for Managing Commonwealth Records Created or Received Using Authentication and Encryption;*[70] and
- *W3C Web Content Accessibility Guidelines.*[71]

---

63 Where possible, common applicable guidelines have been incorporated into the core requirements; however, additional guidelines may need to be incorporated within the Specification to meet the particular business needs of an agency. It is the responsibility of the agency to ensure that all applicable guidelines are addressed within the requirements; the agency must also develop measures to gauge the extent of compliance with this requirement. For more information, refer to the ERMS Guidelines.

64 Defence Signals Directorate, *Australian Government Information and Communications Technology Security Manual* (ACSI 33), March 2005, published online at www.dsd.gov.au/library/infosec/acsi33.html.

65 Department of Finance and Administration, *Commonwealth Procurement Guidelines,* January 2005, published online at www.finance.gov.au/ctc/commonwealth_procurement_guide.html.

66 National Archives of Australia, *Developing a Functions Thesaurus: Guidelines for Commonwealth Agencies*, July 2003, published online at www.naa.gov.au/recordkeeping/control/functions_thesaur/contents.html.

67 National Archives of Australia, *Disaster Preparedness Manual for Commonwealth Agencies,* 2000, published online at www.naa.gov.au/recordkeeping/preservation/disaster/intro.html.

68 National Archives of Australia, *Digital Recordkeeping: Guidelines for Creating, Managing and Preserving Digital Records*, 2004, published online at www.naa.gov.au/recordkeeping/er/guidelines.html.

69 Office of the Privacy Commissioner, *Information Privacy Principles under the Privacy Act 1988*, published online at www.privacy.gov.au/publications/ipps.html.

70 National Archives of Australia, *Recordkeeping and Online Security Processes: Guidelines for Managing Commonwealth Records Created or Received Using Authentication and Encryption*, 2004, published online at www.naa.gov.au/recordkeeping/er/security.html.

71 World Wide Web Consortium (W3C), *Web Content Accessibility Guidelines*, published online at www.w3.org/TR/WCAG.

B. Systems management and design

B.1 Usability

The ERMS must be logical to operate and simple to learn, taking into account the differing needs and abilities of potential users.

User interfaces

B.1.1 The ERMS must provide a user interface that complies with the accepted standard rules for the operating system or platform on which it will operate.[72] (M)

B.1.2 Where the ERMS supports a web browser interface, it must meet Australian Government guidelines for web design, such as *The Guide to Minimum Website Standards* issued by the Australian Government Information Management Office.[73] (R)

B.1.3 The ERMS user interface must be compatible with a range of common accessibility software features[74] and relevant guidelines.[75] (M)

B.1.4 The ERMS may support intuitive navigation using hyperlinks and other cross-references contained in digital records at the time of registration. (D)

B.1.5 The ERMS should support persistent defaults for data entry fields where appropriate, as described in the *Recordkeeping Metadata Standard for Commonwealth Agencies*. (D)

B.1.6 The ERMS must be able to display several digital records and folders simultaneously.[76] (M)

B.1.7 The ERMS should support on-screen tables displaying as pop-up or pull-down menus and pick-lists to assist the entry of metadata. (D)

B.1.8 Where the ERMS employs on-screen windows, it should allow an end-user to re-size or relocate windows, ensuring that content remains correctly aligned within the window. (D)

---

72 Accepted standard rules may be obtained from the official guidelines for the operating system or platform. For example, Apple Computer Inc, *Apple Human Interface Guidelines*, 1992 (rev. 2001–03, 2005), published online at developer.apple.com/documentation/UserExperience/Conceptual/OSXHIGuidelines/OSXHIGuidelines.pdf); and Microsoft Corporation, *Official Guidelines for User Interface Developers and Designers*, 2004, published online at msdn.microsoft.com/library/en-us/dnwue/html/welcome.asp.

73 Australian Government Information Management Office, *The Guide to Minimum Website Standards*, April 2003, published online at www.agimo.gov.au/practice/mws.

74 For examples of common accessibility software features, see The National Archives (UK) *Requirements for Electronic Records Management Systems, 3: Reference Document*, 2002, p. 37, published online at www.nationalarchives.gov.uk/electronicrecords/reqs2002/.

75 For example, see the W3C's *Web Content Accessibility Guidelines*.

76 For example, through the use of tiled or overlapping windows.

B.1.9 Where the ERMS supports a graphical interface, it must allow users to customise it, including: (R)

- menu and toolbar contents;
- screen layout;
- use of function keys;
- on-screen colours, fonts and sizes; and
- confirmations and audible alerts.

B.1.10 The ERMS user interface must be presented consistently across all windows, menus, commands and other facilities. (M)

B.1.11 The ERMS may support advanced features to enhance the usability of the system, such as: (D)

- split-screen display;
- 'drag and drop' manipulation of digital records and folders; and
- multiple user views of the record plan, with no effect on the corporate record plan structure.

Usability of system functions

B.1.12 The ERMS must produce meaningful error messages that offer a simple method of correcting the error or cancelling the process. (M)

B.1.13 The ERMS must ensure that minimal movement between screens is required to perform system operations. (M)

B.1.14 The ERMS should provide an online context-sensitive help facility, including help on the use of the records classification scheme where supported. (D)

B.1.15 The ERMS should support a spell-check facility at all data-entry stages, including searching. (D)

B.1.16 The ERMS must make consistent use of function keys, hot-keys and short-cut keys across all components of the system. (M)

B.1.17 The ERMS must use consistent terminology to label functions and actions in all parts of the system. (M)

B.1.18 The ERMS must be able to hide system functions from users who do not have permission to use them. (M)

B.1.19 The ERMS must prevent users carrying out the initial steps of a process they will be unable to complete due to functional permission restrictions. (M)

B.1.20 The ERMS must support navigation and screen interaction by both mouse and keyboard. (M)

B.1.21 The ERMS should support a logical 'undo' facility for user transactions. (D)

B.1.22 The ERMS must ensure that its facilities are as intuitive and easy to use as possible by allowing: (M)

- functions to be performed with as few mouse clicks or keystrokes as possible; and
- the completion of routine functions from one screen.

B.1.23 The ERMS should provide facilities to assist users with frequently executed operations, such as the: (D)

- ability to define sets of automated consecutive steps; and
- ability to duplicate last entered data.

B.1.24 To allow records to be captured by the ERMS with minimal user intervention, the ERMS must be capable of integrating or interfacing with (as required): (M)

- standard office applications;
- standard electronic messaging systems, such as email clients;
- other mainstream applications already installed; and
- particular business information systems used by the organisation.

B.1.25 The ERMS must be able to generate an electronic message from within the system, in order to attach: (M)

- digital records;
- metadata; and/or
- active pointers to records and/or metadata.

B.2 Reporting

The ERMS must be able to produce reports on system activities and the status of objects within its control, for management, statistical and general purposes.

Report management

B.2.1 The ERMS must provide a reporting capability to produce management, statistical and ad hoc reports on system activity. (M)

B.2.2 The ERMS must be able to restrict an end-user's access to selected reports, or the reporting function in general. (M)

B.2.3 The ERMS must be able to generate reports for screen display and/or printing. (M)

B.2.4 The ERMS should be able to generate reports from multiple databases. (D)

B.2.5 The ERMS must be able to produce ad hoc reports by drawing on relevant information from the audit trail. (M)

B.2.6 The ERMS must allow reports generated to be saved, modified and re-used in the future. (M)

B.2.7 The ERMS should allow authorised users the ability to save generated reports, using one or more common data formats (such as plain text, comma-separated value, or tab-delimited computer file types). (D)

B.2.8 The ERMS must allow reports generated to be easily exported from the system. (M)

Reporting on classification tools

B.2.9 Where the ERMS supports a records classification scheme or business classification scheme, it must be able to generate a report comprising: (R)

- the entire scheme; and
- a part of the scheme (eg a specified function and its related activity terms),

indicating the relationship between terms in a hierarchical format.

B.2.10 Where the ERMS supports a controlled vocabulary, it should be able to generate a report comprising: (D)

- the entire vocabulary; and
- part of the vocabulary (eg specified terms and their related links, or particular entries),

according to relevant standards.[77]

Reporting on folders and records

B.2.11 The ERMS should be able to report the actions carried out on a digital record, or group of records, during a specified date range. (D)

B.2.12 The ERMS should be able to report the actions carried out on a particular folder, or group of folders, during a specified date range. (D)

B.2.13 Where the ERMS supports a records classification scheme or business classification scokey heme, it should be able to report the actions carried out across all or part of the scheme, for a nominated time period. (D)

B.2.14 The ERMS must be able to produce reports listing: (M)

- all folders classified within the records classifications scheme; and
- all folders classified in a section of the records classification scheme,

structured according to the hierarchy of the record plan or other classification tool.

B.2.15 The ERMS must be able to produce statistics for the number and location of digital records by application type and version. (M)

B.2.16 The ERMS must be able to produce statistics for the number and location of digital records and folders by specific access and security controls. (M)

B.2.17 The ERMS must be able to produce a report listing the details and outcome of any migration process, to ensure the integrity of digital records. (M)

B.2.18 The ERMS must be able to report on the size and remaining capacity of its digital record stores and repositories. (M)

Reporting on user activity

B.2.19 The ERMS must be able to report the actions carried out by a particular user, or group of users, during a specified date range. (M)

B.2.20 The ERMS must be able to generate a list of all, or a subset of, user profiles known to the system. (M)

B.2.21 The ERMS must be able to produce statistics for the number of records and folders created by a user or group of users for a defined period. (M)

B.2.22 The ERMS must be able to produce statistics for the number of records viewed by a user or group of users within a defined period. (M)

---

[77] For example, *Documentation – Guidelines for the Establishment and Development of Monolingual Thesauri*, ISO 2788 – 1986, or *Keyword AAA: A Thesaurus of General Terms* (Commonwealth version).

Reporting on access and security

B.2.23	The ERMS must be able to report all attempts at unauthorised access to the System Administrator.	(M)
B.2.24	The ERMS must be able to generate a report based on selected access controls and security controls.	(M)
B.2.25	The ERMS must be able to report on all alterations to access permissions, access controls and security controls, within a specified time period.	(M)
B.2.26	The ERMS must be able to generate a list of all, or a subset of, user access groups known to the system.	(M)

Reporting on disposal activity

B.2.27	The ERMS must be able to produce reports on all disposal activity undertaken by the system.	(M)
B.2.28	The ERMS must be able to produce a report listing: • all disposal classes currently defined in the system; • all digital records, folders or other record plan entities (where supported) to which a particular disposal class is currently applied; • all objects for which a particular disposal action will occur, over a given period of time; and • all objects due for disposal within a given period of time, providing quantitative information on the volume and type of records.	(M)
B.2.29	The ERMS must be able to report on all objects subject to a disposal freeze.[78]	(M)
B.2.30	The ERMS must be able to produce statistics of review decisions over a given period of time.	(M)
B.2.31	The ERMS must be able to produce a report detailing any failure during an export of objects from the system, identifying objects that have generated processing errors or were not successfully exported.	(M)
B.2.32	The ERMS must be able to produce a report detailing the outcome of a destruction process, detailing all objects successfully destroyed and identifying those objects which that were **not** successfully destroyed.[79]	(M)
B.2.33	The ERMS should be able to produce reports to support a transfer process, listing digital records, folders and other record plan entities for transfer according to user-defined metadata elements.	(D)
B.2.34	The ERMS must be able to report on the volume and types of objects that are overdue for disposal.	(M)
B.2.35	The ERMS should be able to produce statistical and graphical reports on disposal activity, within user-specified parameters such as time periods, disposal class or record plan classification.	(D)

[78] A disposal freeze will include objects subject to a pending or ongoing Freedom of Information or legal discovery process, as well as those objects covered by a formal National Archives' disposal freeze.

[79] Conditions for the *successful* destruction of objects are outlined in requirement A.4.53. Destruction of an object is deemed to have been *unsuccessful* if it can still be restored, either partly or totally, after the application of the destruction process outlined in requirement A.4.53.

B.3 System administration

The ERMS must provide facilities for the ongoing maintenance and support of the system, and the data it manages. Some of these functions may be provided by the operating system, database management system or other applications linked to the ERMS.

Data processes

B.3.1	The ERMS must automatically invoke checks that system operations are successfully performed on transactional data.	(M)
B.3.2	The ERMS must support automatic data validation rules.	(M)
B.3.3	The ERMS should accept data transactions carried out online.	(D)
B.3.4	The ERMS should be able to deal with an interrupted data transmission.	(D)
B.3.5	The ERMS may support encrypted transmission between systems.[80]	(D)
B.3.6	The ERMS should be able to support a process for data clean-up.	(D)
B.3.7	The ERMS may support automatic workflow for data transmission processes.[81]	(D)

Deletion of records

(For information on records destruction, see Section A.4, Disposal.)

B.3.8	The ERMS must allow a default or option that prevents any user or System Administrator from changing, moving or deleting in an ad hoc manner a digital record once captured.[82]	(M)
B.3.9	The ERMS must ensure that any function to delete digital records or folders on an ad hoc basis (outside the disposal process) is restricted to the very highest level of System Administrator.[83]	(M)
B.3.10	Where the ERMS allows deletion of a digital record, folder or other record plan entity, it must: • ensure that no objects are deleted if their deletion would result in a change to another object; • notify the System Administrator of any objects linked to the object about to be deleted; • seek confirmation from an authorised user before proceeding with deletion; • delete the entire contents of the object; • record the deletion comprehensively in the audit trail; and • produce an exception report.	(R)
B.3.11	The ERMS must support the retention of metadata for digital records, folders and other record plan entities that have been deleted.	(M)

[80] See Section C.1, Online security.

[81] See Section C.3, Workflow.

[82] Instead, a record might be 'marked' as deleted, and if necessary a pointer or copy placed in the correct location. Alternatively it could be processed for immediate destruction through the authorised disposal mechanism.

[83] Noting requirement A.4.56.

B.3.12 The ERMS must allow a System Administrator to amend user-entered metadata, as part of an audited procedure. (M)

B.3.13 The ERMS must prevent the deletion of metadata that is associated with an object under the control of the system. (M)

Storage

B.3.14 Noting the metadata requirements at A.6.15, the ERMS must support the storage of digital records and associated metadata either: (M)

- together in a digital repository that is an integrated part of the ERMS; or
- separately, with records maintained in the native software environment, and metadata under the control of an ERMS.

B.3.15 The ERMS should have the ability to support the storage of digital records within integrated and distributed storage environments. (D)

B.3.16 The ERMS must provide facilities for monitoring digital repositories. (M)

B.3.17 The ERMS should be able to support online, near-line and off-line storage options for digital records. (D)

B.3.18 The ERMS may be able to support different default digital repositories for different types or classifications of digital records. (D)

B.3.19 The ERMS must be able to prevent or resolve any conflicts caused by changes to storage locations. (M)

B.3.20 The ERMS may be able to support a non-proprietary database. (D)

B.3.21 The ERMS should allow limits to be applied to storage capacities by the System Administrator. (D)

B.3.22 The ERMS must warn a System Administrator when storage limits are about to be reached. (M)

B.3.23 The ERMS may allow the compression of digital records before they are committed to storage. (D)

B.3.24 Where the ERMS supports the compression of digital records, the compression mechanism employed must be integrated with the ERMS. (R)

B.3.25 Where the ERMS supports the compression of digital records, the compression mechanism must be capable of compressing and decompressing the digital records reliably, without any loss or degradation of the record content and metadata, noting B.3.2. (R)

B.3.26 Where the ERMS supports the compression of digital records, the compression functionality must be transparent to users, with compression and decompression of digital records occurring automatically during common processes, such as storage, retrieval, display and export. (R)

B.3.27 The ERMS should support caching of frequently and recently used digital repository content. (D)

B.3.28 The ERMS may support segmentation (and associated hierarchical storage options) for efficient retrieval purposes. (D)

B.3.29 The ERMS should be able to store encapsulated objects. (D)

Back-up and recovery

B.3.30 The ERMS must support automated back-up and recovery facilities for all (or selected) entities, metadata, audit trails and configuration settings held by the ERMS.[84] (M)

B.3.31 The ERMS must support the separate physical storage of back-up data. (M)

B.3.32 The ERMS must allow the manual configuration of frequency of back-ups, and elements of the ERMS to be backed up. (M)

B.3.33 The ERMS must allow a System Administrator to restore the entire ERMS from back-ups, maintaining full data integrity to ensure business continuity. (M)

B.3.34 The ERMS must allow a System Administrator to restore the entire ERMS from the most recent back-up to the point of system failure.[85] (M)

B.3.35 The ERMS must provide notification of any data updates that were unable to be recovered or rebuilt. (M)

B.3.36 The ERMS must support the identification of vital records that are critical to business continuity. (M)

B.3.37 The ERMS should allow vital records to be restored separately from other records. (D)

Preservation

B.3.38 The ERMS must be able to manage digital objects according to the minimum mandatory requirement of this document **over time**, to ensure their integrity and support long-term preservation. (M)

B.3.39 Where the ERMS is expected to manage digital records for a period longer than the anticipated life cycle of the generating application, it must be able to hold and/or generate the preservation metadata as set out in the *Recordkeeping Metadata Standard for Commonwealth Agencies*. (R)

B.3.40 The ERMS must support automatic and manual mapping to and from the ERMS metadata fields. (M)

B.3.41 The ERMS developer must have a program in place to ensure that digital records remain accessible and retain their integrity after a system upgrade. (M)

B.3.42 The ERMS should use widely accepted standards that are the subject of open and publicly available specifications for encoding, storage and database structures. (D)

B.3.43 Where the ERMS uses proprietary encoding, storage or database structures, these must be fully documented, with all documentation available to the System Administrator. (R)

B.3.44 The ERMS must use and house all storage media in environments that are compatible with expected life, and within tolerance of the media manufacturer's specification. (M)

B.3.45 The ERMS must ensure that all tailored modifications are brought forward and are operational when system upgrades are implemented. (M)

B.3.46 The ERMS must be able to migrate digital records, folders and other record plan entities (where supported) in accordance with the requirements for export (A.4.45–A.4.52) and bulk import (A.2.15–A.2.19). (M)

B.3.47 The ERMS must be able to perform a bulk conversion of digital records to other media and/or systems in line with the standards relevant to their format(s). (M)

---

[84] Back-up facility may be built into the ERMS itself, or provided through integration with another system.

[85] For example, using roll-forward, forward-build, RAID or server-clustering methods.

B.3.48 The ERMS should store a converted digital record in both its new and superseded formats, maintaining them as linked objects. (D)

B.3.49 The ERMS should be able to provide event triggers for format conversion at nominated times. (D)

B.3.50 The ERMS should provide an alert to users accessing a converted record, including details about the conversion process such as: (D)

- the original format;
- the new format;
- date of conversion; and
- level of change introduced by the conversion process.

B.3.51 The ERMS must ensure that no data is lost or corrupted during system upgrades, migration or conversion. (M)

B.3.52 The ERMS should support automated comparison of instances of digital records and allow the replacement of any instance found to be corrupted. (D)

B.3.53 The ERMS must support periodic refreshing of storage media, to guard against media degradation. (M)

B.3.54 The ERMS should provide support for the long-term management of encapsulated objects. (D)

B.3.55 The ERMS may provide support for long-term preservation formats, such as archival data formats developed by the National Archives, including:[86] (D)

- the ability to store and manage digital records in archival data formats; and/or
- the ability to convert digital records to archival data formats during capture or export.

B.4 System design

The ERMS design must support response times and levels of system availability that meet current and projected user requirements.

Performance

B.4.1 The ERMS must provide a stable and flexible architecture that can grow to meet changing business needs, and continue to meet the recordkeeping requirements appropriate to its particular implementation. (M)

B.4.2 The ERMS must be able to consistently perform all functions to a specified standard which meets business needs and user expectations. (M)

B.4.3 The ERMS must demonstrate acceptable response times for commonly performed functions, under normal operating conditions.[87] Benchmark measures for performance may include the time taken to: (M)

- display a graphical view of the record plan;
- store standard documents at capture and/or registration;
- return a search response for a simple query;
- return a search response for a complex query;
- display a recently captured record; and
- display a record that has not been accessed for a given period.

[86] Archival data formats have been and continue to be developed by the National Archives as part of its digital preservation strategy.

B.4.4 The ERMS should be able to gather and display performance data. (D)

Scalability

B.4.5 The ERMS must be capable of controlled growth, to continue to meet anticipated organisational needs over time. (M)

B.4.6 The ERMS must demonstrate its capacity to handle the projected needs of the organisation, whilst maintaining the expected performance measurements established at requirements B.4.2–B.4.3.[88] Indicators of scalability may include whether: (M)

- the maximum size of the digital repository will be able to accommodate the expected total number of records;
- the number of geographical locations across which the system will meet anticipated organisational needs;
- the total number of users that can be supported will accommodate predicted staff increases;
- the amount of systems administration and re-configuration down-time required to support projected numbers of records and users during the first five years of operation falls within acceptable parameters; and
- the amount of downtime required to make bulk changes to organisational structures, classification tools and user roles (with the number of folders, records and users anticipated after five years of operation) will fall within specified acceptable parameters.

Reliability and control

B.4.7 The ERMS must demonstrate its capacity to remain available and operational, as required to meet business needs.[89] Measures for reliability may include: (M)

- specified hours of the day, or days of the year, during which the system must be available;
- range of planned or unplanned downtime that can be tolerated; and
- acceptable period of time required to restore the ERMS from back-up in the event of system failure.

B.4.8 The ERMS must have the ability to enforce data integrity, referential integrity and relational integrity at all times. (M)

B.4.9 The ERMS must ensure that all entities (eg folders, records, extracts) are allocated a unique system identifier. (M)

B.4.10 The ERMS should allow a System Administrator to configure the pattern, start and increment of unique system identifiers. (D)

---

87 Performance may be demonstrated through testing, simulation or documentary evidence of independent assessment. Agencies will need to specify measurable values against which to test this requirement authoritatively.

88 Scalability may be demonstrated through testing, simulation or documentary evidence of independent assessment. Agencies will need to specify measurable values against which to authoritatively test this requirement.

89 Reliability may be demonstrated through testing, simulation or documentary evidence of independent assessment. Agencies will need to specify measurable values against which to authoritatively test this requirement.

3. ADDITIONAL FUNCTIONAL REQUIREMENTS

C. Optional functionality

C.1 Online security

The ERMS must be able to manage digital records which have been subjected to online security procedures, and ensure that such processes do not impair the ability of the ERMS to meet the core requirements of this specification.

For more information about the recordkeeping implications of online security technology, refer to the National Archives' guidelines on *Recordkeeping and Online Security Processes*.

Encryption

C.1.1	The ERMS must be able to capture and register an encrypted record directly from an application capable of encryption.	(M)
C.1.2	The ERMS must be able to store digital records in either encrypted or unencrypted form.	(M)
C.1.3	The ERMS must support the use of metadata for digital records transmitted or captured in encrypted form, in accordance with the *Recordkeeping Metadata Standard for Commonwealth Agencies*, including: • the serial number or unique identifier of a digital certificate (where relevant); • type of algorithm and level of encryption; and • date and time stamps relating to encryption and/or decryption processes.	(M)
C.1.4	The ERMS must ensure that an encrypted record can only be accessed by those users associated with the relevant cryptographic key, in addition to other access controls allocated to the record.	(M)
C.1.5	The ERMS must allow encryption to be removed when a record is captured or registered directly from another application.	(M)

Digital signatures

C.1.6	The ERMS must be able to interface with digital signature technologies, so that authentication metadata can be captured automatically.	(M)
C.1.7	The ERMS must be able to check the validity of a digital signature at the time of registering a digital record.	(M)
C.1.8	The ERMS must be able to store with the digital record: • the digital signature associated with that record; • the digital certificate authenticating the signature; and • any other confirmation details, in such a way that they can be retrieved with the record, but without compromising the integrity of a private key.	(M)
C.1.9	The ERMS must support the use of metadata for digital records transmitted or captured bearing digital signatures, in accordance with the *Recordkeeping Metadata Standard for Commonwealth Agencies*. At a minimum this metadata must note that a digital signature was authenticated.	(M)

C.1.10 The ERMS must allow a System Administrator to configure the extent to which authentication metadata is routinely stored with the digital record. For example: (M)
- retain the fact of successful authentication only;
- retain metadata about the authentication process; and
- retain all authentication metadata, including signatures.

C.1.11 The ERMS must be able to demonstrate the continued integrity of a digitally signed record, irrespective of whether authorised changes have been made to its metadata.[90] (M)

C.1.12 During an export process, the ERMS should be able to apply a digital signature to: (D)
- a digital record; and/or
- a digital folder containing multiple records,

in a manner that supports external authentication.

Authentication

C.1.13 The ERMS must be able to store metadata about the process of authentication, including: (M)
- the serial number or unique identifier of the digital certificate;
- the Registration and Certification Authority responsible for authentication; and
- the date and time of authentication.

C.1.14 The ERMS must allow a configuration option to store authentication metadata: (M)
- with the digital record to which it relates; or
- closely but separately linked to the digital record.

C.1.15 The ERMS should provide a flexible architecture in order to accommodate new online security technologies as they are released. (D)

C.1.16 The ERMS must be able to interface with PKI-based security technologies.[91] (M)

Cryptographic key management

C.1.17 The ERMS must support the implementation of a key management plan. (M)

C.1.18 The ERMS must be able to maintain cryptographic keys for the life of the record with which they are associated. (M)

C.1.19 The ERMS must support the separate, secure storage of encrypted records and their associated decryption keys. (M)

C.1.20 The ERMS must be able to store digital certificates for encrypted records and digitally signed records, and must warn a System Administrator of any certificates approaching expiry. (M)

C.1.21 The ERMS must automatically record the details of all online security processes in an audit trail. (M)

C.1.22 The ERMS must support date and time stamping for all records subject to online security processes. (M)

---

[90] Changes may be made to the metadata, but not to the content of the record.

[91] For more information on public key infrastructure, see *Recordkeeping and Online Security Processes.*

Digital watermarks

C.1.23 The ERMS must be able to store records bearing digital watermarks. (M)

C.1.24 The ERMS must be able to store metadata about a digital watermark: (M)

- with the digital record to which it relates; or
- closely but separately linked to the digital record.

C.1.25 The ERMS should be able to retrieve information stored in digital watermarks. (D)

C.1.26 During an export process, the ERMS should be able to apply a digital watermark to: (D)

- a digital record; and
- a digital folder containing multiple records,

in a manner that prevents any loss of access in a receiving system outside the ERMS.

C.2 Document management

The ERMS must be able to provide, or integrate with, document management facilities to ensure records management functions are seamlessly supported.

For more information about records management and document management, refer to the ERMS Guidelines.

Control

C.2.1 The ERMS with document management facilities should allow the management of digital documents (which have not been registered as records) using the same classification tools as those applied to digital records. (D)

C.2.2 The ERMS with document management facilities must make a clear and obvious distinction between digital documents and registered digital records. (M)

C.2.3 The ERMS must provide options for registering all unregistered digital documents in a particular folder or folders as formal records, in a single process. (M)

C.2.4 The ERMS must allow automatic deletion of all unregistered digital documents in a particular folder in one process, or after a set period of time. (M)

Capture

C.2.5 The ERMS with document management facilities should be able to interface with related applications, such as image processing and scanning systems, and workflow systems, while retaining full control of existing records. (D)

C.2.6 The ERMS with document management facilities should be able to automatically capture digital documents and pass them into the ERMS registration process. (D)

C.2.7 The ERMS with document management facilities must be able to capture and register in one process: (M)

- a newly created digital document; and
- a digital document already existing in the document management environment.

C.2.8 The ERMS with document management facilities must be able to capture a digital document and allow the option of completing the registration process at a later time. (M)

C.2.9 The ERMS with document management facilities should be able to register a digital document as a record from within the document management environment. (D)

C.2.10	The ERMS with document management facilities must allow users to transfer smoothly between the document management environment and the ERMS to register a digital document as a record.	(M)
C.2.11	The ERMS with document management facilities should provide a personal workspace, where draft documents can reside until they are either deleted or registered as digital records by the user.	(D)
C.2.12	The ERMS with document management facilities must be able to create versions of digital documents, without automatically creating a new digital record.	(M)
C.2.13	The ERMS with document management facilities must be able to copy a digital record to make a new digital document, ensuring the digital record remains unaffected.	(M)
C.2.14	The ERMS with document management facilities must be able to manage versions in a tightly bound relationship, to support drafting and ensure the integrity of the digital document as a whole.	(M)
C.2.15	The ERMS with document management facilities must provide options for registering some or all versions of a digital document as digital records.	(M)

Access and security

C.2.16	The ERMS with document management facilities should have the ability to apply the same access and security controls to digital documents as are applied to digital records.	(D)
C.2.17	The ERMS with document management facilities must not allow ownership rights[92] from the document management environment to apply to a registered digital record.	(M)
C.2.18	The ERMS with document management facilities must not allow a registered digital record to be checked out, where this would allow the alteration of record content in any way.[93]	(M)

Disposal

C.2.19	The ERMS with document management facilities must be able to detect digital documents in any folder due for export or transfer, and notify the System Administrator.	(M)
C.2.20	The ERMS with document management facilities must enable digital documents to be registered as records prior to export or transfer.	(M)
C.2.21	The ERMS with document management facilities must be able to export only registered digital records.	(M)
C.2.22	The ERMS with document management facilities must automatically destroy digital documents when the digital records to which those documents relate are destroyed subsequent to a successful transfer process.	(M)

[92] For example, rights to edit document content or certain metadata elements, and rights of deletion.

[93] Requirement A.2.27 details the only process by which the content of a registered digital record can be amended.

Searching and retrieval

C.2.23 The ERMS with document management facilities should have the ability to retrieve documents along with records, using the same search interface. (M)

C.2.24 The ERMS should allow an authorised user to configure the retrieval of documents to: (D)

- the latest version only;
- selected versions only;
- only those versions registered as records; or
- all versions of the document.

Metadata

C.2.25 The ERMS with document management facilities must support the mapping of digital document metadata to digital record metadata, as set out in the *Recordkeeping Metadata Standard for Commonwealth Agencies*. (M)

C.2.26 The ERMS with document management facilities must support the definition of templates for common digital documents, and the allocation of a different metadata set for each template.[94] (M)

C.2.27 The ERMS with document management facilities must ensure that any metadata captured in the document management environment is managed in accordance with the requirements of the ERMS Specifications, to ensure its authenticity. (M)

C.2.28 The ERMS with document management facilities must allow metadata to be captured from a user at the time of capture and registration. (M)

C.3 Workflow

The ERMS may provide or be integrated with a workflow facility to support business and records management tasks in a controlled manner. The ERMS must ensure that such processes do not impair its ability to meet the core requirements of this specification.

Workflow features

C.3.1 The ERMS with workflow facilities must support workflows that consist of a number of procedural steps. (M)

C.3.2 The ERMS with workflow facilities must allow standard workflows to be defined and maintained by a System Administrator. (M)

C.3.3 The ERMS with workflow facilities should not limit the number of steps for any given workflow. (D)

C.3.4 The ERMS with workflow facilities must restrict the amendment of pre-programmed workflows to a System Administrator or other authorised user. (M)

C.3.5 The ERMS with workflow facilities must record all changes to pre-programmed workflows in the audit trail. (M)

C.3.6 The ERMS with workflow facilities must recognise both users and workgroups as 'participants'. (M)

C.3.7 The ERMS with workflow facilities should be able to prioritise items in queues. (D)

---

[94] For example, forms, reports and letters.

C.3.8	The ERMS with workflow facilities should allow the receipt of digital records or digital documents to trigger workflows automatically.	(D)
C.3.9	The ERMS with workflow facilities must alert a user when a digital record has been sent to their in-tray for attention, and specify the attention required.	(M)
C.3.10	The ERMS with workflow facilities must support integration with electronic messaging facilities to notify users of records that may be waiting for their attention.	(M)
C.3.11	The ERMS with workflow facilities should allow conditional flows, where the direction of a flow is determined by user input or system data.	(D)
C.3.12	The ERMS with workflow facilities should include 'rendezvous' processing whereby the workflow may be paused pending arrival of a related digital record.	(D)
C.3.13	The ERMS with workflow facilities may support sequential and parallel routing.	(D)
C.3.14	The ERMS with workflow facilities must track the progress of a digital record or folder through a workflow, so a user can determine its status in the process.	(M)
C.3.15	The ERMS with workflow facilities should enable participants to view queues of work addressed to them, and select items to work on.	(D)
C.3.16	The ERMS with workflow facilities should support the distribution of incoming items across workgroups, in order to balance group workloads.	(D)
C.3.17	The ERMS with workflow facilities should provide a reminder, or 'bring forward' facility for digital records and folders.	(D)

Workflow management

C.3.18	The ERMS with workflow facilities must not limit the number of workflows that can be defined.	(M)
C.3.19	The ERMS with workflow facilities should allow the System Administrator to allocate permissions to other users or groups, so that they may reassign tasks or actions in a workflow.	(D)
C.3.20	The ERMS with workflow facilities should manage digital records in queues that can be examined and controlled by the System Administrator.	(D)
C.3.21	The ERMS with workflow facilities should allow an authorised user to indefinitely suspend and then continue a workflow.	(D)
C.3.22	The ERMS with workflow facilities should associate time limits with individual steps in each flow and report items that are overdue according to these limits.	(D)
C.3.23	The ERMS with workflow facilities must provide comprehensive reporting facilities to allow the monitoring of volumes, performance, and exceptions.	(M)

Workflow and records management

C.3.24	The ERMS with workflow facilities must ensure digital records and folders remain correctly classified during a workflow process, retaining all links to other record plan entities.	(M)
C.3.25	The ERMS with workflow facilities must allow a digital document to be captured and registered during, or at the conclusion of, a workflow process.	(M)
C.3.26	The ERMS with workflow facilities must maintain the same access and security controls that apply to digital records and folders at all other times.	(M)
C.3.27	The ERMS with workflow facilities must ensure that workflow processes do not interfere with the scheduled disposal of digital records and folders.	(M)
C.3.28	The ERMS with workflow facilities must notify a System Administrator that a digital record or folder within a workflow process is due for disposal.	(M)

C.3.29	The ERMS with workflow facilities must ensure that digital records and folders within workflow process can be located using the standard search interface.	(M)
C.3.30	The ERMS with workflow facilities must support the progressive addition of metadata to digital records and folders, as set out in the *Recordkeeping Metadata Standard for Commonwealth Agencies*.	(M)

C.4 Hybrid system management

The ERMS must support the management of markers, physical folders and hybrid folders in a manner consistent and fully integrated with the management of digital records and folders.

For more information about hybrid systems, refer to the ERMS Guidelines.

Control and capture

C.4.1	The ERMS must support the management of markers, physical folders and hybrid folders in a manner consistent with the management of digital records and folders.	(M)
C.4.2	The ERMS must allow physical folders to be classified with the same records classification tools in the same record plan used to manage digital folders.	(M)
C.4.3	The ERMS must allow hybrid folders, which are part digital and part physical, to be classified with the same records classification tools in the same record plan used to manage digital folders.	(M)
C.4.4	The ERMS must allow the physical and digital components of a hybrid folder to use the same title and unique identifier, but with appropriate indicators marking which is physical and which is digital.	(M)
C.4.5	The ERMS must enable the creation of a marker for each physical record registered in the ERMS.	(M)
C.4.6	The ERMS must allow markers to denote different types of physical record, allowing a user to enter the format as descriptive metadata.	(M)
C.4.7	The ERMS must allow markers to be classified with the same records classification tools in the same record plan used to manage digital records.	(M)

Access and security

C.4.8	The ERMS must ensure that the physical and digital components of a hybrid folder are allocated the same access and security controls.	(M)
C.4.9	The ERMS must maintain the same access and security controls for markers, physical folders and hybrid folders that apply to digital records and folders at all times.[95]	(M)

Disposal

C.4.10	The ERMS must support the application of a disposal class to a physical folder, in a manner consistent with the management of digital folders.	(M)
C.4.11	The ERMS must ensure that the physical and digital components of a hybrid folder are allocated the same disposal class.	(M)
C.4.12	The ERMS must ensure that the disposal action carried out on a hybrid folder is applied to both physical and digital components at the same time, taking into account the different processes required for destruction where applicable.	(M)

[95] Noting requirement B.3.38.

C.4.13	The ERMS must apply disposal review decisions to both the physical and digital components of a hybrid folder.	(M)
C.4.14	The ERMS must ensure that destruction or transfer of a digital folder results in the destruction of any markers contained in that folder.	(M)
C.4.15	The ERMS must maintain minimum metadata for destroyed items, including markers, physical folders and hybrid folders.[96]	(M)
C.4.16	The ERMS must alert the System Administrator to the existence and location of the physical component of a hybrid folder, when such a folder is due for export or transfer.	(M)
C.4.17	The ERMS must allow the export of physical folders and hybrid folders, retaining all associations with the digital component of the hybrid folder[97] and the record plan once they are exported.	(M)
C.4.18	The ERMS must allow the export of markers, retaining all associations with digital records and folders once they are exported.	(M)
C.4.19	The ERMS must require a System Administrator to confirm that the physical component of a hybrid folder has been transferred, exported or destroyed before the digital component of the folder can be processed.	(M)

Searching and retrieval

C.4.20	The ERMS must be able to retrieve markers, physical folders and hybrid folders along with digital records and folders, using the same search interface.	(M)
C.4.21	The ERMS must ensure that retrieval of a digital folder also retrieves all markers associated with that folder.	(M)
C.4.22	The ERMS must ensure that when a hybrid folder is retrieved, its physical and digital components are also retrieved.	(M)
C.4.23	The ERMS should support the production and use of barcodes tracking and locating physical folders and physical records.	(D)
C.4.24	The ERMS should enable the tracking of physical folders and records by providing check-in and check-out facilities that record: • the check-out location of the item;[98] and • the dates of check-out and check-in.	(D)
C.4.25	The ERMS should be able to reveal the tracking history of a physical folder or record to a System Administrator or other authorised user upon completion of a search. This history should include the following information: • current location; • previous locations; and • associated dates.	(D)
C.4.26	The ERMS should support a bring-forward facility for physical folders and records, allowing a user to enter a reserve date for an item and transmitting a message to the user or a System Administrator for action.	(D)
C.4.27	The ERMS should support an ordering facility, allowing a user to request a physical folder or record already checked-out by another user or located in a storage area.	(D)

---

[96] Where supported, see requirement A.4.69.

[97] As applicable.

[98] Location may be a physical location, a workgroup or user.

Metadata

C.4.28	The ERMS must support the use of metadata for markers, physical folders and hybrid folders, including inheritance of metadata consistent with inheritance by a digital record or folder.	(M)
C.4.29	The ERMS should support the capture and display of metadata for markers, physical folders and hybrid folders, as set out in the *Recordkeeping Metadata Standard for Commonwealth Agencies*.	(D)
C.4.30	The ERMS must allow a different metadata element set to be configured for markers, physical folders and hybrid folders than that for digital records and folders so that metadata for physical entities can include physical location information.	(M)
C.4.31	The ERMS must record changes to location metadata in the audit trail.	(M)

GLOSSARY

Definitions that do not have citation details are new definitions provided by the National Archives. The sources of other definitions are noted.

Term	Definition
Access	The right, opportunity, means of finding, using or retrieving information, usually subject to rules and conditions. Access to Commonwealth records for agencies and the public is governed by the *Archives Act 1983*. Under the Act, there is a general right of access to Commonwealth records that are in the open period, subject to certain exemptions. Sources: Adapted from AS ISO 15489, Part 1, Clause 3.1; International Council on Archives, ISAD (G), p. 14; National Archives of Australia, *Glossary of Recordkeeping Terminology*, 2004.
Access controls	A scheme of non-hierarchical mechanisms, which may be applied to digital records and record plan entities 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 controls** and **User access group**. Source: Adapted from The National Archives (UK), *Requirements for Electronic Records Management Systems, 3: Reference Document*, 2002, p. 28.
Active metadata	Metadata available for use by the ERMS to support or trigger automated records management processes. See also **Metadata** and **Descriptive metadata**..
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 upon 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**. Source: National Archives of Australia, *Glossary of Recordkeeping Terminology*, 2004.
Aggregation	Any accumulation of record entities at a level above record object (document, digital object),eg digital folder, series. See also **Folder** and **Record category**.
AGLS	The Australian metadata standard (AS 5044.1) for the discovery and retrieval of government information online. Formerly known as Australian Government Locator Service. See also **Metadata** and **Recordkeeping metadata**. Source: National Archives of Australia, *Glossary of Recordkeeping Terminology*, 2004.
Application programming interface (API)	An application program(ing) 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. Source: Archives New Zealand, *Electronic Recordkeeping Systems Standard*, June 2005, p. 14.
Archival data format	A format into which digital data objects are converted for long-term preservation. Source: National Archives of Australia, *Digital Recordkeeping: Guidelines for Creating, Managing and Preserving Digital Records,* 2004.

Term	Definition
Archives	Records that are appraised as having archival value. Note: This definition of the term 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.' Sources: Ellis, J (ed), *Keeping Archives*, 2nd edition, Australian Society of Archivists, Thorpe Melbourne 1993, p. 463; *IBM Dictionary of Computing*, McGraw Hill, New York, 1994 p. 30; National Archives of Australia, *Glossary of Recordkeeping Terminology*, 2004 and *Digital Recordkeeping: Guidelines for Creating, Managing and Preserving Digital Records,* 2004.
Audit trail	Data that allows the reconstruction of a previous activity, or which enables attributes of a change (such as date, time, operator) to be stored so that a sequence of events can be determined in the correct chronological order. Usually in the form of a database or one or more lists of activity data. Sources: Adapted from The National Archives (UK), *Requirements for Electronic Records Management Systems, 3: Reference Document*, 2002, p. 1.
Australian Governments' Interactive Functions Thesaurus (AGIFT)	A web-based thesaurus that enables users to search online government resources. The thesaurus links natural language terms with terms used by governments. Source: National Archives of Australia, *Glossary of Recordkeeping Terminology*, 2004.
Authentication	The process of establishing that the sender of a message is who he/she claims to be. Source: National Archives of Australia, May 2004, *Recordkeeping and Online Security Processes: Guidelines for Managing Commonwealth Records Created or Received Using Authentication and Encryption*.
BCS	See **Business classification scheme**.
BIS	See **Business information system**.
Browsing	Method of finding a record by starting at a known point and following linked terms and other identified paths to locate required information. Source: Adapted from New South Wales Department of Public Works and Services, *Request for Tender No. ITS2323 for the Supply of Records and Information Management Systems*, March 2001, Part B - Specifications, p. 12.
Business classification scheme (BCS)	1. A conceptual representation of the functions and activities performed by an organisation. The scheme is derived from the analysis of business activity (as in Step B of DIRKS). 2. The business classification scheme is the basis from which classification tools, such as a functions thesaurus and records classification scheme, are developed. See also **Disposal authority** and **Records classification tool**. Source: National Archives of Australia, *Glossary of Recordkeeping Terminology*, 2004.

Term	Definition
Business information system (BIS)	1. Organised collection of hardware, software, supplies, policies, procedures and people, which stores, processes and provides access to an organisation's business information. 2. 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, finance or human resources systems. See also **Electronic document management system (EDMS), Electronic records management system (ERMS)** and **System**. Sources: National Archives of Australia, *Glossary of Recordkeeping Terminology*, 2004. Adapted from AS 4390, Part 1, Clause 4.17.
Capture	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 information systems so that the capture of records is concurrent with the creation of records. See also **Registration**. Sources: National Archives of Australia, Glossary of Recordkeeping Terminology, 2004, and Digital Recordkeeping: Guidelines for Creating, Managing and Preserving Digital Records, 2004. Adapted from AS 4390, Part 1, Clause 4.7.
Certification Authority	A body that generates, signs and issues public key certificates which bind subscribers to their public key Source: National Archives of Australia, May 2004, *Recordkeeping and Online Security Processes: Guidelines for Managing Commonwealth Records Created or Received Using Authentication and Encryption*.
Checksum	An algorithm-based method of determining the integrity and authenticity of a digital data object. Used to check whether errors or alterations have occurred during the transmission or storage of a data object. Source: National Archives of Australia, *Digital Recordkeeping: Guidelines for Creating, Managing and Preserving Digital Records,* 2004.
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 **Security classification system**. Sources: National Archives of Australia, *Glossary of Recordkeeping Terminology*, 2004. Adapted from AS ISO 15489, Part 1, Clause 3.5; AS 4390, Part 1, Clause 4.8.
Classification system	A set of terms and business rules that can be applied to records to facilitate capture, control, retrieval, maintenance and disposal. Source: National Archives of Australia, *Glossary of Recordkeeping Terminology*, 2004.
Classification tools	See **Records classification tool**.

Term	Definition
Commonwealth record	A record that is the property of the Commonwealth or of a Commonwealth institution; or a record that is deemed to be a Commonwealth record by virtue of a regulation under the *Archives Act 1983*, but does not include a record that is exempt material or is a register or guide maintained in accordance with the Act. See also **Record**. Source: National Archives of Australia, *Glossary of Recordkeeping Terminology*, 2004. Adapted from *Archives Act 1983*, Part I, Section 3.
Component	Set of constituent parts that comprise 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 – eg for migration purposes. See also **Digital object** and **Digital record**. 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 digital objects. For example, a web page with embedded graphics and style sheets. Source: Archives New Zealand, *Electronic Recordkeeping Systems Standard*, June 2005, p. 14.
Control	The physical and/or intellectual management established over records by documenting information about their physical and logical state, their content, their provenance, and their relationships with other records. The systems and processes associated with establishing control include registration, classification, indexing, and tracking. See also **Classification**, **Indexing**, and **Registration**. Source: National Archives of Australia, *Glossary of Recordkeeping Terminology*, 2004.
Controlled copy	An exact reproduction of a digital record, where the ERMS ensures there is no change to the content of the record. A controlled copy may be allocated to a different part of the record plan but must be linked to the originating record and all other controlled copies of that record.
Controlled vocabulary	Alphabetical list containing terms or headings which are authorised or controlled so that only one heading or form of heading is allowed to represent a particular concept or name. See also **Indexing** and **Thesaurus**. Sources: Adapted from Kennedy, J and Schauder, C, *Records Management: A Guide to Corporate Recordkeeping*, 2nd edition, Longmans, Melbourne, 1988, p. 291.
Conversion	The process of changing records from one medium to anther 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** and **Rendition**. Sources: National Archives of Australia, *Glossary of Recordkeeping Terminology*, 2004. Adapted from AS ISO 15489, Part 1, Clause 3.7 and Part 2, Clause 4.3.9.2.
Cryptographic key	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. See also **Encryption**, **Key management plan (KMP)** and **Public key infrastructure (PKI)**. Source: National Archives of Australia, May 2004, *Recordkeeping and Online Security Processes: Guidelines for Managing Commonwealth Records Created or Received Using Authentication and Encryption*.

Term	Definition
Data	Facts or instructions represented in a formalised manner, suitable for transmission, interpretation or processing manually or automatically. Source: National Archives of Australia, *Digital Recordkeeping: Guidelines for Creating, Managing and Preserving Digital Records*, 2004. Adapted from the International Council on Archives, *Dictionary of Archival Terminology*, KG Saur, Munich, 1988 p. 48.
Deletion	The process of removing, erasing or obliterating recorded information from a medium outside the disposal process. Deletion within electronic systems generally refers to the removal of the pointer (ie location information) that allows the system to identify where a particular piece of data is stored on the medium. Deletion does not meet the requirements for destruction of Commonwealth records as it may be possible to retrieve the deleted data before it is completely over-written and obliterated by the system. See also **Destruction** and **Disposal**.
Descriptive metadata	Metadata that is available for informational purposes only (such as comments and notes fields), and is not actively used by the ERMS to support or trigger automated records management processes. See also **Active metadata**.
Descriptor	Non-hierarchical qualifier (eg 'Personnel') attached to a security category to limit access to particular records. Descriptors may be informative or advisory but cannot actively control access. See also **Descriptive metadata**. Source: Adapted from The National Archives (UK), *Requirements for Electronic Records Management Systems, 3: Reference Document*, 2002, pp. 27–28.
Destruction	1. The process of eliminating or deleting records, beyond any possible reconstruction. 2. In this specification, 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 the National Archives of Australia. See also **Deletion** and **Disposal**. Sources: National Archives of Australia, *Glossary of Recordkeeping Terminology*, 2004. Adapted from AS ISO 15489, Part 1, Clause 3.8.
Digital certificate	An electronic document signed by the Certification Authority which: identifies a key holder and the business entity he or she represents; 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, May 2004, *Recordkeeping and Online Security Processes: Guidelines for Managing Commonwealth Records Created or Received Using Authentication and Encryption*.
Digital document	A document created and/or maintained by means of digital computer technology. See also **Document**.
Digital folder	A set of related digital records held in a tightly bound relationship within the ERMS and managed as a single object. May also be referred to as a container. See also **Folder**.
Digital object	An object that can be represented by a computer, such as a file type generated by a particular system or software application (eg a word-processed document, a spreadsheet, an image). A digital record may comprise one or more digital objects. See also **Component** and **Digital record**.

Term	Definition
Digital record	A record created, and/or maintained by means of digital computer technology. Includes records that are 'born digital' or have undergone conversion from a non-digital format. Digital records are a subset of electronic records. See also **Electronic record** and **Record**.
Digital repository	A direct access device on which digital records and their associated metadata are stored. A repository may be an integrated part of the ERMS, or a separate storage area under the ERMS control. Source: Adapted from Department of Defense (US), *Design Criteria Standard for Electronic Records Management Software Applications, DoD 5015.2-STD*, June 2002, p. 17.
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*, 2004; Australian Government Information Management Office, *Trusting the Internet – A Small Business Guide to E-security*, July 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 Interchange of Documentation between Administrations Programme), *Model Requirements for the Management of Electronic Records* (MoReq Specification), March 2001, p. 70.
DIRKS	The acronym for 'designing and implementing recordkeeping systems', a methodology for managing records and other business information that is outlined in the *Australian Standard for Records Management*, AS ISO 15489, Part 1, Section 8.4) and elaborated in the 2001 National Archives' publication, *The DIRKS Manual: A Strategic Approach to Managing Business Information*. Source: National Archives of Australia, *The DIRKS Manual: A Strategic Approach to Managing Business Information*, September 2001.
Disposal	Any action that changes the circumstances of a record or removes a record from its usual setting. Disposal can include destruction, damage, alteration, or transfer of custody or ownership of records. The National Archives of Australia authorises disposal of Commonwealth records for the purposes of the *Archives Act 1983*. Also called disposition, usually in the North American context. See also **Disposal authority**. Source: National Archives of Australia, *Glossary of Recordkeeping Terminology*, 2004.
Disposal action	The action noted in a disposal authority indicating the minimum retention period for a record and the event from which the disposal date should be calculated. See also **Disposal trigger** and **Retention period**. Source: National Archives of Australia, *Glossary of Recordkeeping Terminology*, 2004.

Term	Definition
Disposal authority	1. A formal instrument that defines the retention periods and consequent disposal actions authorised for classes of records described in the authority. 2. Section 24 of the *Archives Act 1983* empowers the National Archives to authorise the disposal of Commonwealth records. Records disposal authorities (RDAs) apply to the records of a single organisation, while general disposal authorities (GDAs), such as the Administrative Functions Disposal Authority, normally apply to all Commonwealth agencies. See also **Disposal action**, **Disposal class** and **Retention period**. Sources: National Archives of Australia, *Glossary of Recordkeeping Terminology*, 2004. Adapted from *Archives Act 1983,* Part V, Division 2, Section 24; AS 4390, Part 1, Clause 4.10.
Disposal class	A description of the characteristics of a group of records documenting similar activities, together with a disposal action to be applied to the group. The description consists of function and activity terms and scope notes, record description and disposal action. Component of a disposal authority, implemented within an ERMS as a set of rules made up of a disposal trigger, a retention period and a disposal action, which may be applied to a record plan entity. Source: National Archives of Australia, *Glossary of Recordkeeping Terminology*, 2004.
Disposal freeze	1. A ban on disposal action that applies to certain groups of records as designated by the National Archives of Australia from time to time. 2. Mechanism within an ERMS that can prevent any disposal action from taking place, even if the retention period for a digital record has elapsed. The disposal freeze mechanism may be applied to prevent the disposal of records identified as being subject to a pending or ongoing Freedom of Information or legal discovery process, or records identified as being subject to a formal National Archives disposal freeze. Information on current National Archives' disposal freezes is available at www.naa.gov.au/recordkeeping/disposal/freezes.html Source: National Archives of Australia, *Glossary of Recordkeeping Terminology*, 2004.
Disposal trigger	The point from which the disposal action is calculated. This can be a date on which action is completed or a date on which an event occurs. See also **Retention period**. Source: National Archives of Australia, *Glossary of Recordkeeping Terminology*, 2004.
Document (noun)	Recorded information or object that can be treated as a unit. See also **Record**. Sources: National Archives of Australia, *Glossary of Recordkeeping Terminology*, 2004; AS ISO 15489 – 2002, Part 1, Clause 3.10.
EDMS	See **Electronic document management system**.

Term	Definition
Electronic document management system (EDMS)	An automated system used to support the creation, use and maintenance of electronically created documents for the purposes of improving an organisation's workflow. These systems do not necessarily incorporate recordkeeping functionality and the documents may be of informational rather than evidential value (ie the documents may not be records). EDMS are a subset of business information systems whose primary purpose is to support creation, revision and management of digital documents. See also **Business information system (BIS)**, **Electronic records management system (ERMS)** and **System**. Source: National Archives of Australia, *Digital Recordkeeping: Guidelines for Creating, Managing and Preserving Digital Records,* 2004.
Electronic messages	Any communication using an electronic system for the conduct of official business internally, between Australian Government agencies, or with the outside world. Common examples include email, instant messaging and SMS (short messaging services). Source: National Archives of Australia, *Digital Recordkeeping: Guidelines for Creating, Managing and Preserving Digital Records,* 2004.
Electronic messaging systems	Applications used by agencies or individuals for sending and receiving, as well as storing and retrieving, electronic messages. These systems generally do not possess recordkeeping functionality Source: National Archives of Australia, *Digital Recordkeeping: Guidelines for Creating, Managing and Preserving Digital Records,* 2004.
Electronic record	A record created, communicated and/or maintained by means of electronic equipment. Although this term can refer to analogue materials (eg videotapes), it generally refers to records held in digital form on magnetic or optical computer storage media. See also **Digital record**. Source: Adapted from *Standards Australia AS 4390*, Part 1, Clause 4.13; Kennedy, J, and Schauder, C, *Records Management: A Guide to Corporate Recordkeeping*, 2nd edition, Longmans, Melbourne, 1988, p. 293.
Electronic records management system (ERMS)	An automated system used to manage the creation, use, maintenance and disposal of electronically created records for the purposes of providing evidence of business activities. These systems maintain appropriate contextual information (metadata) and links between records to support their value as evidence. ERMS are a subset of business information systems whose primary purpose is the capture and management of digital records. See also **Business information system (BIS)**, **Electronic document management system (EDMS)** and **System**. Source: National Archives of Australia, *Digital Recordkeeping: Guidelines for Creating, Managing and Preserving Digital Records,* 2004.
Encapsulated object	Digital records that have been 'packaged' with enough metadata to preserve their content and context, and to support their reconstruction at some time in the future. The encapsulated metadata is managed as an integral part of the record. Source: Adapted from National Archives of Australia, *Digital Recordkeeping: Guidelines for Creating, Managing and Preserving Digital Records,* 2004.

Term	Definition
Encryption	The process of converting data into a secure code, through the use of an encryption algorithm, for transmission over a public network. The mathematical key to the encryption algorithm is encoded and transmitted with the data, thus providing the means by which the data can be decrypted at the receiving end and the original data restored. Sources: National Archives of Australia, *Digital Recordkeeping: Guidelines for Creating, Managing and Preserving Digital Records,* 2004; Australian Government Information Management Office, *Trusting the Internet – A Small Business Guide to E-security*, July 2002, p. 43.
ERMS	See **Electronic records management system**.
Export	A disposal process, whereby copies of a digital record (or group of records) are passed with their metadata from one system to another system – either within the organisation or elsewhere. Export does not involve removing records from the first system. See also **Transfer**. Source: Adapted from The National Archives (UK), *Requirements for Electronic Records Management Systems, 3: Reference Document*, 2002, p. 3.
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.
Extraction	The act of creating an extract. See also **Extract**.
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. See also **Folder**. **Note**: For the purposes of the ERMS Specification, 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. Sources: Ellis, J (ed), *Keeping Archives*, 2nd edition, Australian Society of Archivists, Thorpe Melbourne 1993, p. 470; and National Archives of Australia, *Glossary of Recordkeeping Terminology*, 2004.
File plan	See **Record plan**.
Folder	An aggregation of records represented in an ERMS and allocated to a records category within the records classification scheme. A folder is constituted of metadata which may be inherited from the parent (records category) and passed on to a child (record). See also **Digital folder**, **Physical folder** and **Hybrid folder**. Source: Adapted from The National Archives (UK), *Requirements for Electronic Records Management Systems, 3: Reference Document*, 2002, p. 3.
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*, June 2002, p. 14.

Term	Definition
Function	The first level of a business classification scheme. Functions represent the major responsibilities that are managed by the organisation to fulfil its goals. They are high-level aggregates of the organisation's activities. Sources: National Archives of Australia, *Glossary of Recordkeeping Terminology*, 2004. Adapted from AS 4390, Part 4, Clause 7.2.
Government public key infrastructure (GPKI)	Collective term for the standards, products, services and service providers certified under the Gatekeeper strategy. It also refers to the policies created for the management of those standards, products, services, and the relationships between them. See **Public key infrastructure (PKI)**. Source: National Archives of Australia, National Archives of Australia, *Recordkeeping and Online Security Processes: Guidelines for Managing Commonwealth Records Created or Received Using Authentication and Encryption,* May 2004.
Hybrid folder	A set of related digital folders and physical folders. Both folders are held in a tightly bound relationship within the ERMS and managed as a single object. Records managed within a hybrid folder deal with the same subject, activity or transaction. See also **Folder**. Source: Adapted from The National Archives (UK), *Requirements for Electronic Records Management Systems, 3: Reference Document*, 2002, p. 4.
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,* 2004.
Import	To receive digital records and associated metadata into one system from another, either within the organisation or elsewhere.
Indexing	The process of establishing access points to facilitate retrieval of records and/or information. Source: National Archives of Australia, *Glossary of Recordkeeping Terminology*, 2004.
Inherit	To take on a metadata attribute from a parent entity. See also **Retrospective inheritance**. 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.
Integration	A tightly bound relationship between the ERMS and another application or mechanism. Integration implies data being shared between systems, a common look and feel that suggests a single application. Source: Adapted from New South Wales Department of Public Works and Services, *Request for Tender No. ITS2323 for the Supply of Records and Information Management Systems*, Part B – Specifications, March 2001, p. 13.

Term	Definition
Interface	A mechanism whereby data can be exchanged between applications. Source: Adapted from New South Wales Department of Public Works and Services, *Request for Tender No. ITS2323 for the Supply of Records and Information Management Systems*, Part B – Specifications, March 2001, p. 13.
Key management plan (KMP)	A strategy to ensure continuing access to public and private key pairs. Describes how cryptographic services are securely deployed within an organisation, documents critical controls to protect keys and associated material during their life, along with other controls to provide confidentiality, integrity and availability of keys. See also **Cryptographic key** and **Public key infrastructure (PKI)**.
Keyword AAA	A thesaurus of general terminology designed for use in the Australian public sector for classifying, titling and indexing administrative records in most technological environments. It covers administrative terminology common to most organisations and should be used in conjunction with a functions thesaurus relating to the organisation's specific functions to provide comprehensive controlled vocabulary coverage. It was developed by the Archives Authority of New South Wales. The National Archives of Australia has developed a Commonwealth version of Keyword AAA – *Keyword AAA: A Thesaurus of General Terms* (Commonwealth version) – which is available to Commonwealth agencies under a whole-of-government licence. Further information on the National Archives of Australia, *Keyword AAA: A Thesaurus of General Terms* (Commonwealth version), 2001, is available at www.naa.gov.au/recordkeeping/control/KeyAAA/summary.html. Source: National Archives of Australia, *Glossary of Recordkeeping Terminology*, 2004.
Marker	Metadata profile of a record physically held outside the ERMS. 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). **Note**: A paper file will usually be represented and managed in the ERMS as a physical folder. It is not envisaged that a physical folder would contain markers for each document or record place on a paper file. Source: Adapted from The National Archives (UK), *Requirements for Electronic Records Management Systems, 3: Reference Document*, 2002, p. 4.
Metadata	Structured information that describes and/or allows users to find, manage, control, understand or preserve other information over time. See also **Active metadata** and **Descriptive metadata**. Sources: National Archives of Australia, *Glossary of Recordkeeping Terminology*, 2004; Cunningham, A, 'Six degrees of separation: Australian metadata initiatives and their relationships with international standards', *Archival Science*, vol. 1, no. 3, 2001, p. 274.
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. See also **Conversion**. Sources: National Archives of Australia, *Glossary of Recordkeeping Terminology*, 2004; AS ISO 15489 – 2002, Part 1, Clause 3.13 and Part 2, Clause 4.3.9.2.

Term	Definition
Naming principle	Rule for labelling digital records and other record plan entities. May include titling conventions, the use of a controlled vocabulary or indexing scheme and the allocation of textual or alphanumeric references.
Native format	The format in which the record was created, or in which the originating application stores records. See also **Conversion**. Source: Adapted from New South Wales Department of Public Works and Services, *Request for Tender No. ITS2323 for the Supply of Records and Information Management Systems, Part B – Specifications*, March 2001, p. 13.
Participant	Any party involved in a particular business process for the purposes of a workflow. A participant may be a system user, business work group or software application.
Physical folder	An entry in the record plan for a hardcopy (usually paper) folder. The folder itself is stored outside the ERMS but metadata about its location and management is maintained in the system. A physical folder may stand on its own within the records classification scheme, or it may form part of a hybrid folder 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 or photograph. See also **Marker, Physical folder** and **Record**.
Protective marking	See **Security category**.
Public key infrastructure (PKI)	The combination of hardware, software, people, policies and procedures needed to create, manage, store and distribute keys and certificates based on public key cryptography. See also **Cryptographic key**, **Digital certificate** and **Government Public Key Infrastructure**. Source: National Archives of Australia, *Recordkeeping and Online Security Processes: Guidelines for Managing Commonwealth Records Created or Received Using Authentication and Encryption*, May 2004.
Record	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. Sources: National Archives of Australia, *Digital Recordkeeping: Guidelines for Creating, Managing and Preserving Digital Records,* 2004; AS 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 (records category) and passed on to a child (folder). The full set of record categories, at all levels, together constitutes the records classification scheme. A record category does not itself contain records; it is an attribute against which a folder is classified. See also **Records classification scheme**. Source: Adapted from The National Archives (UK), Requirements for Electronic Records Management Systems, 3: Reference Document, 2002, p. 1.
Record plan	The records classification scheme plus all the folders. Also called a file plan. See also **Folder** and **Records classification scheme**. Source: Adapted from The National Archives (UK), *Requirements for Electronic Records Management Systems, 3: Reference Document*, 2002, p. 3.

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.
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). Sources: National Archives of Australia, *Glossary of Recordkeeping Terminology*, 2004; AS 4390, Part 1, Clause 4.19; AS 4390, Part 3, Foreword.
Recordkeeping metadata	Structured or semi-structured information that enables the creation, management and use of records through time and across domains. Recordkeeping metadata can be used to identify, authenticate and contextualise records, and the people, processes and systems that create, manage and maintain and use them. See also **Active metadata** and **Metadata**. Sources: National Archives of Australia, *Glossary of Recordkeeping Terminology*, 2004; Wallace, D, 'Archiving Metadata Forum: Report from the Recordkeeping Metadata Working Meeting, June 2000', *Archival Science*, vol. 1, no. 3, 2001, p. 255.
Recordkeeping 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. Also called a Records system. Sources: National Archives of Australia, *Glossary of Recordkeeping Terminology*, 2004. Adapted from AS 4390, Part 3, Clause 6.2.1.
Records classification scheme	A hierarchical classification tool which, when applied to a business information system, can facilitate the capture, titling, retrieval, maintenance and disposal of records. A records classification scheme stems from an organisation's business classification scheme. See also **Record plan**. Source: National Archives of Australia, *Glossary of Recordkeeping Terminology*, 2004.
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.

Term	Definition
Records management	The field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposal of records, including processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records. Sources: National Archives of Australia, *Glossary of Recordkeeping Terminology*, 2004. Adapted from AS ISO 15489, Part 1, Clause 3.16.
Records management system	See **Recordkeeping system**.
Referential integrity	Ensuring that all references are updated or deleted as necessary when a key reference is changed in a database environment. Source: Adapted from Department of Defense (US), *Design Criteria Standard for Electronic Records Management Software Applications, DoD 5015.2-STD*, June 2002, p. 16.
Register	See **Registration**.
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. Source: National Archives of Australia, *Glossary of Recordkeeping Terminology*, 2004. Adapted from AS ISO 15489, Part 1, Clause 3.18; AS 4390, Part 1, Clause 4.24.
Relational integrity	Ensuring that subordinate (or 'child') objects are updated or deleted as necessary when a superior (or 'parent') object is changed. Preventing 'orphans'. Source: Adapted from Department of Defense (US), *Design Criteria Standard for Electronic Records Management Software Applications, DoD 5015.2-STD*, June 2002, p. 17.
Rendition	Instance of a digital record made available in another format or on different medium by a process entirely within the ERMS 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. See also **Conversion**.
Request for tender (RFT)	A published notice inviting businesses who satisfy the conditions for participation to submit a tender in accordance with requirements of the request for tender and other procurement documentation. Source: Department of Finance and Administration, *Guidance on the Mandatory Procurement Procedures*, January 2005, p. 67.
Retention period	The length of time after the disposal trigger that a record must be maintained and accessible. At the expiration of the retention period, a record may be subject to disposal. See also **Disposal action** and **Disposal trigger**.
Retrospective inheritance	Process whereby a subordinate (or 'child') entity automatically takes on a metadata attribute from its superior (or 'parent') entity when (a) the metadata of the parent entity is changed; or (b) the child entity is moved from one parent entity to another. Source: Adapted from The National Archives (UK), *Requirements for Electronic Records Management Systems, 3: Reference Document*, 2002, p. 4

Term	Definition
Review	1. A disposal process, whereby a folder or group of records is examined to consider the allocation of a disposal class or whether any disposal action can take place. 2. An assessment process undertaken to evaluate the effectiveness, appropriateness, relevance and efficiency of an identified system, or systems. Source: Adapted from The National Archives (UK), *Requirements for Electronic Records Management Systems, 3: Reference Document*, 2002, p. 6.
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 in accordance with the *Commonwealth Protective Security Manual* issued by the Attorney-General's Department. 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), March 2001, p. 107.
Security classification system	A set of procedures for identifying and protecting official information, the disclosure of which could have adverse consequences for the Commonwealth. 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: National Archives of Australia, *Glossary of Recordkeeping Terminology*, 2004. 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 in accordance with the *Commonwealth Protective Security Manual*. May include a hierarchical security category, possibly in conjunction with a non-hierarchical qualifier. See also **Access controls** and **Descriptor**.
Sentencing	1. The process of identifying the disposal class a record belongs to and applying the disposal action specified in the relevant disposal authority to the record. 2. In an ERMS, sentencing refers to the allocation of a disposal class to a particular digital record or folder. Source: National Archives of Australia, *Glossary of Recordkeeping Terminology*, 2004.
System	1. A set of interrelated components that work together to achieve some common purpose. 2. The term 'system' is commonly used to describe computer software applications. However, software is also supported by an infrastructure of users, administrators, policies, procedures, rules and associated tools which can be used to meet the requirements in this Specification. See also **Business information system (BIS)**, **DIRKS**, **Electronic document management system (EDMS)**, and **Electronic records management system (ERMS)**, and **Recordkeeping system**.
System access control	Any mechanism used to prevent access to the ERMS by unauthorised users. May include the definition of user profiles, or the use of ID and password login. See also **Access controls** and **Security controls**.

Term	Definition
System administrator	A user role with designated responsibility for configuring, monitoring and managing the ERMS 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.
Thesaurus	1. In a thesaurus, the meaning of the 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: National Archives of Australia, *Glossary of Recordkeeping Terminology*, 2004. Adapted from AS 4390, Part 4, Clause 7.3.2.2; AS ISO 15489, Part 2, Clause 4.2.3.2.
Tracking	Creating, capturing and maintaining information about the movement and uses of records. Sources: National Archives of Australia, *Glossary of Recordkeeping Terminology*, 2004. Adapted from AS ISO 15489, Part 1, Clause 3.19.
Transaction	1. The smallest unit of business activity. Uses of records are themselves transactions. 2. The third level in an business classification scheme. See also **Activity**, **Business classification scheme** and **Function**. Source: National Archives of Australia, *Glossary of Recordkeeping Terminology*, 2004. Adapted from AS 4390, Part 1, Clause 4.27, and AS ISO 15489, Part 2, Clause 4.2.2.2.
Transfer	A disposal process, consisting of a confirmed export of digital records and folders, followed by their destruction within the exporting ERMS. Records may be transferred from one Commonwealth agency to another following administrative change, from a Commonwealth agency to archival custody, from a Commonwealth agency to a service provider, from the Commonwealth 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.
User access group	Discrete set of named individuals (users known to the ERMS) that make 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 profile	A summary of all attributes allocated to a user of the ERMS. 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 ERMS 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.

Term	Definition
Vendor	1. A person or company selling or supplying goods and services. 2. In relation to the ERMS market, the term vendor usually relates to companies responsible for the development and sale of ERMS software.
Vital records	Records without which an organisation could not continue to operate; that is, those containing information needed to re-establish the organisation in the event of a disaster. Vital records are those that protect the assets and interests of the organisation as well as those of its clients and shareholders. Source: National Archives of Australia, *Glossary of Recordkeeping Terminology*, 2004. Adapted from Kennedy, J, and Schauder, C, *Records Management: A Guide to Corporate Recordkeeping*, 2nd edition, Longman, Melbourne, 1988, p. 302.
Web-based records	A generic term that refers to all types of web-based information that meets the criteria of a record, including public websites, virtual private networks, extranets and intranets. Source National Archives of Australia, *Digital Recordkeeping: Guidelines for Creating, Managing and Preserving Digital Records,* 2004.
Workflow	The automation of a business process, in whole or in part, during which documents, information or tasks are passed from one participant to another for action, according to a set of procedural rules. A participant may be a system user, business work group or software application. Source: Workflow Management Coalition, *The Workflow Management Coalition Specifications: Workflow Management Coalition Terminology and Glossary*, WFMC–TC–1011, February 1999, p. 8.
Workgroup	See **Participant**.
XML (eXtensible Markup Language)	A simple, flexible computer language developed by the World Wide Web Consortium as an open, non-proprietary technology that creates common information formats so that both the format and the data can be shared between organisations, regardless of their respective Internet computing platforms. Source: National Archives of Australia, *Digital Recordkeeping: Guidelines for Creating, Managing and Preserving Digital Records*, 2004. Adapted from Australian Government Information Management Office, *B2B E-Commerce: Capturing Value Online*, 2001, p. 90.