This document is no longer current. Please go to the following URL for more information:

http://www.nationalarchives.gov.uk/electronicrecords/reqs2002/default.htm

the national archives

Requirements for Electronic Records Management systems

3: Reference Document

July 2007 Revision

Requirements for
Electronic Records Management systems

1: Functional Requirements

2: Metadata Standard

3: Reference Document

4: Implementation Guide

The National Archives
Ruskin Avenue
Kew
Surrey
TW9 4DU
United Kingdom

e-mail: e-records@nationalarchives,gov.uk
Website: www.nationalarchives.gov.uk/electronicrecords

© Crown copyright 2002 - 2007

3: Reference Document

Foreward 6

Glossary of Terms 7

Key For Figures 23

Entity Relationships 26

- Acceptable Entity Relationships 26
- Unacceptable Entity Relationships 27
- Parent and Child Fileplan Object Relationships 28
- Relationship between an unrelated electronic and physical folder 29
- Underlying Hybrid Folder Relationship 30
- Hybrid Folder Relationship 32
- Record Relationships 33

Description of Entities 34

Entity Life Histories 40

- folder entity life history 40
- Folder Creation 41
- Folder Management 42
- Folder Disposal 44
- Commentary: Folders 45
  - *Key Concepts 45*
  - *Life history events 45*
- Electronic record entity life history 50
- Record Creation 51
- Manage Record 52
- Record Disposal 53
- Commentary: Records 54
  - *Key concepts 54*
  - *Life history events 54*
- Generic Disposal Schedule Process 57

Example Disposal Schedules 59

Access Control Model 60

- Hierarchical access control 60
- Security categories 61
- Example of hierarchical access controls 61
- Descriptors 62
- Non-hierarchical access control 63
- Interaction of access controls 63

User Roles 64

User Metadata Elements 67

Flat listing of Metadata Elements 68

FOLDER LEVEL METDATA ELEMENTS 70
PART LEVEL METADATA ELEMENTS 72
RECORD LEVEL METADATA ELEMENTS 72
E-MAIL TRANSMISSION DATA MAPPING 75
COMPONENT LEVEL METADATA ELEMENTS 75

Sample Accessibility Guidelines 76

Mapping of Functional Requirements and Terminology 78

MAPPING OF TNA REQUIREMENTS TO MOREQ AND DOD 78
TNA: 1999 Requirements which are not mapped to any TNA: 2002 Requirement in the main table 92
MoReq requirements which are not mapped to any TNA: 2002 Requirement in the main table 92
DoD 5015.2:2002 requirements which are not mapped to any TNA: 2002 requirement in the main table 93
Mapping of TNA, MoReq, and DoD Terminology 93

Bibliography 95

UK LEGISLATION 95
RELEVANT STANDARDS DOCUMENTS 95
OTHER REFERENCES 96

FOREWARD

This document forms part of a series of publications issued by The National Archives under the broad title of Requirements for Electronic Records Management Systems. This document entitled the "Reference Document" is an updated version of volume 3 in the series.

When these documents were first published, there were 4 volumes:

- Volume 1: Functional Requirements
- Volume 2: Metadata Standard
- Volume 3: Reference Document
- Volume 4: Implementation Guidance

In January 2005, an additional module was added to provide requirements for casework and workflow systems. The entire series is available on the website of The National Archives at:

http://www.nationalarchives.gov.uk/electronicrecords/reqs2002/default.htm

This Reference document is intended to assist public authorities, ERMS integrators and vendors to understand how the main functional requirements published in volume 1 and the record management metadata standard in volume 2 relate to one another and to provide additional guidance on interpreting the record management model defined in those requirements.

The document was first published in 2002 but with the closure of the related software testing scheme in August 2006 an opportunity has been taken to revise and extend the Reference Document.

As with the first edition the document aims to explain the basic concepts using:

- a detailed glossary
- provide relevant relationship models for fileplan objects.
- Entity descriptions
- an access control model
- mapping functional requirements to requirements to other international standards for example the Model Requirements for Electronic Records Management issued by the European Commission in 2001 (MoReq) and the US Department of Defense record management standard DOD 5015.2 2002.

However the development of this revision has also used this opportunity to respond to requests for additional guidance by providing a far more extensive set of entity diagrams and related commentaries, which have added significantly to the size of the document.

GLOSSARY OF TERMS

This glossary defines key terms used in the Requirements for Electronic Records Management systems 2002, The Metadata Standard, and this Reference Document.

Some definitions are closely adapted from:

- The terms and definitions in ISO 15489 standard for records management.
- The glossary in BSI BIP0008 2004 Code of Practice for Legal Admissibility.

Where appropriate, references to these publications are indicated by a footnote.

access control list – see custodian and role

The ERMS must support use of access control markings which identify:

- pre-defined groups of users, and separately
- individual users,

in order to control which users are allowed access to which electronic records, folders and classes.[1]

Access to fileplan objects can be controlled in a number of ways. Access control lists specify which individual ERMS user(s) or group(s) should be able to access particular objects.

For example, where a personnel folder exists in an ERMS it is not desirable for every user to view it. It is, however, necessary for the HR department and the appropriate individual to view it. An ERMS System Administrator can configure the access control lists for a folder so that access is given to both an HR group and individual users as appropriate whilst preventing others from accessing the folder.

aggregation – see classification scheme and fileplan

Concept of record assemblies existing within a fileplan classification i.e. classes, folders, parts and records are the basic form of aggregation. Element **10. Aggregation** in the records management metadata standard discusses aggregation as a metadata attribute.

[1] *Functional Requirement A.5.10M, Requirements for Electronic Records Management Systems 2002*

audit trail

Data which allows the reconstruction of a previous activity, or which enables attributes of a change (such as date / time, operator) to be stored[2] so that a sequence of events can be reconstructed in their correct chronological sequence.

The ERMS must be able to record an audit trail of events under the control of the ERMS, storing information about:

- the action which is being carried out
- the object(s) to which the action is being applied
- the user carrying out the action
- the date and time of the event[3]

capture – see declaration

Capture and declaration are the terms used to describe the way in which an electronic document that exists outside of the main ERMS environment can be processed so that it becomes a record within the ERMS classification scheme.

Essentially capture is the point at which a copy of an electronic document is added to the ERMS data repository, with appropriate system and user metadata closely bound to the document. If the capture process can be performed independently, then suitably authorised users will typically be able to edit the document and specified metadata via the ERMS interface.

child object – see inheritance and parent object

An object held one level lower than another in the hierarchy is a child object. For example, a folder is the child of the class that it is allocated to. Child objects will often inherit key metadata from their parent object, for example disposal schedule and access controls.

class – see folder

A class is a subdivision of an electronic classification scheme by which the electronic fileplan is organised. A class may either be sub-divided into one or more lower level classes, or may have a child folder; classes and folders will never be present at the same level of a hierarchical branch of the fileplan. A class does not contain records.

classification [1] – see classification scheme

A systematic identification of business activities (and thereby records) into categories according to logically structured conventions, methods and procedural rules represented in a classification scheme.[4]

---

[2] *British Standards Institution BSi DISC PD0008: 1999 Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically*

[3] *Functional Requirement A.6.1M, Requirements for Electronic Records Management Systems 2002*

[4] *International Standards Organisation ISO 15489 Information and Documentation: Records Management, 2 vols. 2001*

classification [2] – see protective marking and security category

A scheme of protective security markings used to control access to classes, folders and records.

In an attempt to minimise potential confusion, the term "classification" is not used in the context of security categories within the scope of this publication.

Note: See the Access Control Model on page 60 for further detail.

classification scheme – see aggregation, classification [1] and fileplan

An intellectual structure (sometimes referred to as a business classification scheme (BCS)) that categorises records to preserve their context relative to other objects within a fileplan. The full set of classes, at all levels, together constitute the classification scheme. No assumptions are made about the principles of the division, which might be based on functions, activities and subjects, or themes and sub-themes.

Further guidance and information on different ways of constructing a BCS can be found in "The National Archives Business Classification Scheme Design" guidelines, and also ISO15489 2003. See Bibliography on page 95.

component – see document, electronic record and record

The smallest aggregation of data managed by an operating system, also referred to in computer terminology as a "file". Within the scope of these requirements, the term "component" is used when referring to document or record content.

A record may be comprised of one or more components. An example of typical one-component record content is a single, stand-alone spreadsheet. An example of multi-component record content is a webpage that is comprised of HTML and separate image components.

Typical end users will not be able to interact directly with the individual components - i.e. users would normally engage with the content from the document or record level.

Components must be properly maintained by an ERMS so that associated properties are recorded and managed as required over time, e.g. for migration purposes. Components must be retrievable and displayed in the same manner as observed in their original format. Figure 1.5 on page 33 illustrates the relationship of a standard electronic record to its components and other instances of the record that may be created.

Note: the term "component" has been defined as such for the Requirements for Electronic Records Management systems 2002; it is not in widespread use elsewhere.

custodian – see access control list

A custodian is either a single user or named group of users with responsibility for a particular set of records at a particular time, typically a case officer or departmental records manager.

cut-off date – see part

A fixed period, or recurring date, which specifies the date when an existing part should be automatically closed, and a new part opened. For example, an annual cut-off at the end of each financial year.

Data Protection Act 1998 (c.29)

The Data Protection Act 1998 (c.29) came into force on 1 March 2000. Under the Data Protection Act, anyone processing personal information must comply with eight principles of good information handling. The eight principles state that personal data must be:

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate and up to date.
- Not kept longer than necessary.
- Processed in accordance with the individual's rights.
- Secure.
- Not transferred to countries outside the European Economic area, unless there is adequate protection.

See Bibliography on page 95.

declaration – see capture, document and record

Capture and declaration are the terms used to describe the way in which an electronic document that exists outside of the main ERMS / EDRMS environment can be processed so that it becomes a record within the ERMS / EDRMS classification scheme.

Capture is the point at which a copy of an electronic document is added to the ERMS / EDRMS data repository, with appropriate system and user metadata closely bound to the document.

Declaration is the point at which the document (i.e. record content) and specified metadata elements are frozen so that they cannot be edited by any user, thereby ensuring the integrity of the original data as a complete, reliable and authentic record. The declaration process formally passes the data into corporate control.

destroy – see disposal schedule, metadata stub and transfer

The process of eliminating records beyond any possible reconstruction.[5]

Destroy is a managed disposal action for the total removal of fileplan objects from the ERMS and underlying database. When fileplan objects are destroyed, it might be desirable to retain a metadata stub in their place.

Destruction as a managed disposal action should not be confused with deletion, which would allow suitably authorised users to remove data on an ad-hoc basis as part of a controlled and audited action.

[5] *International Standards Organisation ISO 15489 Information and Documentation: Records Management, 2 vols. 2001*

disposal schedule – see destroy, export, review and transfer

A disposal schedule is a set of rules that may be allocated to a class, folder, or specific non-default record_type definition, to determine the length of time for which a fileplan object should be retained by the organisation for business purposes, and the eventual fate of the affected object(s) on completion of the retention period.

Disposal schedules will include:

- A triggering event, such as the closure of a folder.
- A retention period, such as 6 years and 2 months.
- A disposal action, such as review, export, transfer, or destroy.

document – see component, declaration, electronic document, physical document and record

Recorded information, stored on a physical medium, which can be interpreted in an application context and treated as a unit.[6]

A document may be held on paper, microform, magnetic, or other electronic and physical medium. A document may include any combination of text, data, graphics, sound, moving pictures or any other forms of information. A document may consist of one or more components.

A document consists of both content (i.e. one or more components) and metadata. While documents can be edited and deleted, records are held in a fixed state, with appropriate access and functional permissions applied.

EDRMS – see capture and ERMS

EDRMS is an acronym for electronic document and record management system. An EDRMS is a software application that is capable of capturing and managing electronic documents alongside electronic records.

e-GIF / e-Government Interoperability Framework

Published by the e-Government Unit, formally the Office of e-Envoy, e-GIF provides technical policies and specifications to government departments. In particular, the framework is a standard for UK public sector information systems to promote interoperability. It incorporates the e-GMF / e-GMS metadata standard. See Bibliography on page 95.

e-GMS / e-Government Metadata Standard – see metadata, Metadata Standard and records management metadata standard

A qualified Dublin Core metadata scheme published by the Office of the e-Envoy within the e-GIF. The e-Government Metadata Standard (e-GMS) lays down the elements, refinements and encoding schemes to be used by government officers when creating metadata for their information resources or when designing search systems for information systems. The e-GMS forms part of the e-GIF. See Bibliography on page 95.

Note: The Requirements for Electronic Records Management systems 2002 make use of version 2.0 of the Metadata Standard. Version 3.0 of the standard was published in 2004.

[6] *International Standards Organisation ISO 15489 Information and Documentation: Records Management, 2 vols. 2001*

EIR / Environmental Information Regulations 1992 (S.I. 1992/3240) – see Freedom of Information Act 2000 (c.36)

Statutory instrument, under the European Communities Act 1972 (c.68), giving a statutory right of access to information about the environment (subject to certain exemptions).

Note: S.I. 1992/3240 has subsequently been revoked with savings by Environmental Information Regulations S.I. 2004/3391. See Bibliography on page 95.

electronic document – see document and electronic record

A document in electronic form.

An electronic document is information generated using any form of software. Examples include text-based documents generated by a word processor, spreadsheets, graphics and images, HTML / XML documents, multimedia documents, etc.

An electronic document may consist of one or more components.

An electronic document consists of both content (i.e. one or more components) and metadata. While electronic documents can be edited and deleted, electronic records are held in a fixed state, with appropriate access and functional permissions applied

electronic folder – see electronic part and folder

An electronic folder is a (virtual) container for related records. Electronic folders (segmented into electronic parts) exist solely in the ERMS environment and may contain one or more electronic records or markers. In the ERMS hierarchy, folders are represented by metadata profiles that include relevant informative and functional data for the folder (and its contents).

electronic part – see electronic folder and part

An electronic part is a segment of an electronic folder; it has no existence independent of the electronic folder. An electronic folder will always contain at least one electronic part, the first part, and (unless a second part is created) it is co-extensive with the whole folder. Under normal operating conditions, only the most recent part will be open at any given time.

Note: strictly speaking, records are contained within a segmented part, although an ERMS interface may present records as though they were contained directly within a folder.

electronic record – see component, electronic document, marker and record

An electronic record is an electronic document which has been formally declared as a corporate record.

A typical electronic record consists of both electronic content (one or more components) and metadata. While electronic documents can be edited and deleted, electronic records are held in a fixed state, with appropriate access and functional permissions applied.

Due to the nature of electronic records, the "Location" metadata elements will not have a value (other than "null").

Note: Markers may exist alongside electronic records in the fileplan. Markers are electronic metadata profiles, which can be used to represent physical records within the ERMS environment

element – see metadata, Metadata Standard, sub-element and refinement

A metadata field applied to any object. A number of the fields set out in the Metadata Standard operate at the same level as in resource discovery metadata schemes and can be applied directly to records management entities (e.g. **3. Title** or **4. Subject**). However, in a records management scheme most of the elements are applied to objects at the sub-element level (e.g. the sub-elements of **6. Date** include "**Date.Declared**", "**Date.Opened**" and "**Date.Closed**".)

Note: This is necessary to achieve a scheme that supports the processes of electronic records management with the necessary precision. Semantically, it would perhaps be more accurate to call these “elements” in their own right (as in MoREQ and PRO 1999). However, the terminology of the e-GMS has been preferred at this level to aid comparison between the two Standards. The "elements" in these cases serve more as logical groupings for the purposes of the record management Metadata Standard.

encoding scheme

Possible or permissible values forming a controlled vocabulary / set of authority terms for an "element" or "sub-element". As most records management metadata is system derived, the encoding scheme should be defined in system configuration. A scheme may be created using an official standard, such as the e-Government Metadata Standard, but this may have to be adapted in order to address the specific needs of an organisation.

entity – see object

The term "entity" is largely synonymous with "object", and the two terms are used interchangeably within this Reference Document. Both terms refer to any object within an ERMS. It is not in itself a functional aspect of an ERMS but a descriptive term.

Both terms are more often used to refer to fileplan objects (e.g. class, folder, part, and record), but "entity" and "object" can be used to refer to various aspects of an ERMS.

ERMS – see capture and EDRMS

ERMS is an acronym for electronic record management system. An ERMS is a software application that is used to capture / declare and manage electronic records throughout their lifetime.

export – see disposal schedule and transfer

Export is a managed disposal action for passing copies of fileplan object metadata and content (as applicable) from one ERMS to another specified destination. Export (as opposed to transfer) does not remove the exported objects from the source ERMS, and should be a repeatable process.

extract – see redaction

An extract is a copy of a record, from which some material may have been removed or permanently masked (redacted). An extract is often made when the full record cannot be released, for example under the Freedom of Information Act 2000 (c.36), but part of the record can.

Historically, in the paper environment, an extract referred to material removed from a record in the process of making a redaction**.** This concept can be applied in the electronic environment where the physical storage of an extract as a secure redacted version can be created either as a version of the original that is tightly bound to it, or is stored as a separate record within the ERMS. The terms extract and redaction are often treated as synonymous but in this glossary have been separated for clarity.

Note: some advanced systems may allow extract components to be tightly bound within the originating record. The ERMS functionality would manage the whole record in an appropriate manner, applying strict access controls and viewing functionality to ensure that users only have access to the appropriate aspects of the record.

file

This term is not used in isolation in order to avoid confusion between ERMS and general operating system terminology.

fileplan – see aggregation and classification scheme

The full set of classes, folders and records together make up a fileplan. It is a full representation of an organisation, designed to support the conduct of the business, and meet records management needs.

folder – see class, electronic folder, hybrid folder, physical folder and part

A folder is a container for related records. Folders (segmented into parts) are the primary unit of management and may contain one or more records (or markers where applicable). Folders are allocated to a class. See figure 1.0 on page 26.

Where the term "folder" is used in isolation, it may refer to all folder types, i.e. electronic, hybrid and physical. The term can also be qualified to specify the nature of the folder..

Freedom of Information Act 2000 (c.36) – see EIR / Environmental Information Regulations 1992 (S.I. 1992/3240)

The Freedom of Information Act 2000 (c.36) came fully into force on 1 January 2005. This act deals with access to official information (subject to certain exemptions).

hybrid folder – see folder, and hybrid part

Hybrid folders are created within the ERMS in order to manage situations where related material exists in both electronic and physical formats.

The electronic aspect of a hybrid folder is a (virtual) container for related records and markers. Within the ERMS environment, hybrid folders (segmented into hybrid parts) provide the metadata profiles for related electronic and physical data. The electronic and physical aspects of a hybrid folder must be managed as one. See figure 1.3 and figure 1.4 on pages 30 and 32 respectively.

Note: The display of hybrid folders may vary from ERMS to ERMS. Some ERMS products may display both electronic and physical objects in the same view; others may alternate between the display of an electronic folder and physical folder, providing a method to toggle between them.

hybrid part – see hybrid folder and part

Hybrid folders (segmented into hybrid parts) are created within the ERMS in order to manage situations where related material exists in both electronic and physical formats.

A hybrid part is a segment of a hybrid folder; it has no existence independent of the hybrid folder. A hybrid folder will always contain at least one hybrid part, the first part, and (unless a second part is created) it is co-extensive with the whole folder.

Under normal operating conditions, only the most recent part will be open at any given time.

Note: strictly speaking, records are contained within a segmented part, although an ERMS interface may present records as though they were contained directly within a folder.

inheritance – see child object and parent object

The principle by which some of a child object's metadata value(s) are populated by those of its parent object, by either:

- **Inheritance on creation**
- By default, he child object is given the value(s) of a metadata attribute from the parent object upon creation.

- **Retrospective inheritance**
- When the parent object metadata value(s) has been changed (e.g. by editing a specific field or by moving the object within the fileplan), the inherited metadata for the child object is automatically updated to match that of the parent.

marker – see electronic record, physical record and record

Markers are electronic metadata profiles, which can be used to represent physical records within the ERMS environment in a similar manner to standard electronic records.

Unlike electronic records, markers have no electronic content.

Due to the nature of markers, the "Location" metadata elements must be populated in order to provide details regarding the physical location of the object. See figure 1.3 and figure 1.4 on pages 30 and 32 respectively.

Within the scope of these requirements, markers are only expected to be assigned to electronic folders (either standard electronic folders or to the electronic aspect of hybrid folders). It is not envisaged that markers will be assigned to physical folders in the ERMS environment.

metadata – see e-GMS / e-Government Metadata Standard, element and sub-element

Metadata can be defined as data about data. Essentially, metadata is data that describes the context, content and structure of all fileplan objects identified in the ERMS environment.

The Metadata Standard provides a detailed list of elements and their sub-elements where applicable, for all fileplan objects. Standard rules and principles govern the management of metadata throughout an object's lifetime.

Metadata Standard - see e-GMS / e-Government Metadata Standard and element

Within the scope of this publication, the e-Government Metadata Standard is often referred to simply as the "Metadata Standard".

metadata stub – see destroy and transfer

When a fileplan object is destroyed as part of a disposal process it may be desirable to retain selected metadata in order to provide historic data for management purposes. If a metadata stub is retained, the ERMS must be able to clearly differentiate between existing and destroyed objects within the fileplan.

The minimum set of records management metadata standard elements to be retained for class, folder and part objects is as follows:

- The unique identifiers of the fileplan object.
- The fileplan object's title.
- The open and close dates of folders and parts.
- The disposal schedule ID, the due / effective date, as well as who authorised the disposal and any comments they may have made.

Whilst this is the minimum metadata set that should be retained, depending on business needs an organisation may chose to retain other metadata values.

migration

The process of moving records from one technological platform to another, to refresh software or media formats, while maintaining their authenticity, integrity, reliability and usability.[7]

As software applications become obsolete, it is vital that record content in older electronic formats can still be accessed and viewed.

MoREQ / Model Requirements for Recordkeeping 2000

Requirements for EDRM produced by an EC-funded project; not specific as to sector or format. An updated version of these requirements is due to be published in 2007. As of July 2007, www.dlm-network.org provides more detail on the current status of this revision. See Bibliography on page 95.

object – see entity

The term "object" is largely synonymous with "entity", and the two terms are used interchangeably within the Reference Document. Both terms refer to any object within an ERMS. It is not in itself a functional aspect of an ERMS but a descriptive term.

Both terms are more often used to refer to fileplan objects (e.g. class, folder, part, and record), but "entity" and "object" can be used to refer to various aspects of an ERMS.

parent object – see child object and inheritance

An object held one level higher than another in the hierarchy is a parent object. For example, a class is the parent object of a folder that is placed within it. Parent objects will often provide key metadata to their child objects via inheritance, for example disposal schedule and access controls.

part – see cut-off date, electronic part, folder, hybrid part and physical part

A part is a segment of a folder; it has no existence independent of the folder. A folder will always contain at least one part, the first part, and (unless a second part is created) it is co-extensive with the whole folder. Parts allow the contents of folders to be grouped and disposed of in a regular and orderly manner without need for closing the whole folder.

Under normal operating conditions, only the most recent part will be open at any given time.

Note: strictly speaking, records are contained within a segmented part, although an ERMS interface may present records as though they were contained directly within a folder.

permanent preservation

The process by which records are preserved in perpetuity in an accessible and reliable form. Permanent preservation ensures that they are maintained as authentic records, reflecting their business context and use.

[7] *International Standards Organisation ISO 15489 Information and Documentation: Records Management, 2 vols. 2001*

physical document – see document and physical record

Physical documents exist in the physical, non-electronic environment. Within the ERMS environment.

A physical document may be held as paper, microform, magnetic or any other physical medium (e.g. laboratory samples, video cassettes, etc.). A physical document may include any combination of text, data, graphics, sound, moving pictures or any other forms of information.

Similar to electronic documents, physical documents have content and metadata (i.e. context). While documents can be edited and deleted, records are held in a fixed state, with appropriate access and functional permissions applied.

Note: In theory, the concept of markers could be expanded to cater for physical documents as well as physical records but that it beyond the scope of this publication.

physical folder – see folder, and physical part

A physical folder is a container for related records. Physical folders (segmented into physical parts) exist in the physical, non-electronic environment and may contain one or more physical records.

Within the ERMS environment, metadata profiles can be used to represent physical folders in a similar manner to standard electronic folders.

There are two scenarios where a physical folder may be represented within an ERMS:

- where the physical folder stands on its own, and has no relationship with an electronic folder in the ERMS, other than being allocated to the same classification level
- where the physical folder is directly related to an electronic folder in the ERMS, and shares the same title; the physical and electronic folder together constitute a hybrid folder.

Due to the nature of physical folders, the "Location" metadata elements must be populated in order to provide details regarding the physical location of the object.

See figure 1.2 on page 29. It may also be desirable to create a custom metadata field for the format of the folder to be captured (i.e. a paper wallet, lever arch binder).

physical part – see part and physical folder

Physical parts exist in the physical, non-electronic environment. Within the ERMS environment, metadata profiles can be used to represent physical parts in a similar manner to standard electronic parts.

Within the ERMS, a segmented physical part has no existence independent of the physical folder. A physical folder (e.g. representing a paper file in the physical environment) will always contain at least one physical part, the first part, and (unless a second part is created) it is co-extensive with the whole folder.

Under normal operating conditions, only the most recent part will be open at any given time.

Note: strictly speaking, records are contained within a segmented part, although an ERMS interface may present records as though they were contained directly within a folder.

physical record – see marker, physical document and record

Physical records exist in the physical, non-electronic environment. Within the ERMS environment, metadata profiles (i.e. markers) can be used to represent physical records.

A physical record may be held as paper, microform, magnetic or any other physical medium (e.g. laboratory samples, video cassettes, etc.). A physical record may include any combination of text, data, graphics, sound, moving pictures or any other forms of information.

Similar to electronic records, physical records have content and metadata (i.e. context). While documents can be edited and deleted, records are held in a fixed state, with appropriate access and functional permissions applied.

pointer

A pointer is a method of creating multiple instances of an electronic record in more than one folder without physical duplication of the record. More than one pointer can be created within the fileplan to reference a single record, but each pointer must be managed as a separate record in its own right.

Where used, a pointer should provide a means of identifying the location of both the originating record and any other pointers. These links should not be static shortcuts but should retain their integrity by always pointing to the originating record even if that record is relocated within the fileplan.

presentation

Process of publishing folders, records and their metadata for 'presentation' outside the ERMS environment (e.g. for publication on a website) by methods within ERMS control. The presentation data must be rendered in a form suitable for publication as opposed to simply being bare textual data or tagged raw system data.

protective marking – see classification [2], role and security category

Protective marking is a metadata field applied to an object to show the level of security assigned to the object. A protective marking is selected from a predefined set of possible values which indicate the level of access controls applicable to a folder, record etc. within the fileplan hierarchy.

Within the scope of these requirements, there are 5 standard security categories, ranging from "Unclassified" to "Top Secret".

Note: See the separate descriptions of protective markings in the Access Control Model on page 60 for further detail.

record – see component, declaration, document, electronic record, physical record and record type

Information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business.[8]

In the Requirements for Electronic Records Management systems 2002, a record is a document that has been formally declared into an ERMS. Records can only be allocated to a folder within an ERMS (with the record held within the currently open segmented part of the folder).

A record consists of both content (i.e. one or more components) and metadata. While electronic documents can be edited and deleted, electronic records are held in a fixed state, with appropriate access and functional permissions applied.

record_type – see record

A definition of a record object with specific metadata attributes that will dictate particular behaviour for any record associated with that record_type. A default record_type is the norm, while a non-default, specific record_type is a deviation from the norm. In particular this concept is used for the purposes of complying with the fair processing provisions of the Data Protection Act 1998 (c.29) to enable different disposal behaviour of records created as instances of a limited number of pre-defined record_types.

records management metadata standard - see e-GMS / e-Government Metadata Standard

Within the scope of this publication, the e-Government Metadata Standard is often referred to as the records management metadata standard.

redaction – see extract

In the paper world, a redaction is created when some material is removed or obscured. The same term is sometimes applied to the creation of extracts in the electronic world, where certain record information is either masked or deleted prior to it being released.

Note: The terms "extract" and "redaction" are often treated as synonymous but in this glossary have been separated for clarity.

refinement – see element and sub-element

Refinement is a term used in a qualified Dublin Core metadata schemes (including e-GMS) to 'refine' the meaning of the main metadata element applied to an object.

For the purposes of the Metadata Standard, the term "sub-element" is used to describe this level. This is seen as semantically more suitable for the function of these attributes, many of which will apply to the same entity, whilst not implying a narrower scope than the main element.

[8] *International Standards Organisation ISO 15489 Information and Documentation: Records Management, 2 vols. 2001*

rendition

A rendition is an instance of a record rendered into another software format by a process entirely within the control of the ERMS, without loss of content. The content and most of the metadata (i.e. all except the relational linking back to the native format record and details of the software format) are identical. Renditions may be required for preservation or access / viewing purposes.

Note: Some advanced systems may allow extract components to be tightly bound within the originating record. The ERMS functionality would manage the whole record in an appropriate manner, applying strict access controls and viewing functionality to ensure that users only have access to the appropriate aspects of the record.

resource discovery

Generic description of the activity of information retrieval, usually in the electronic environment.

review – see disposal schedule

Review is a managed disposal action for examining the metadata (including disposal schedule status) of a class, folder, part or record to ascertain whether a final disposal can be determined where this has not previously been possible (i.e. that it should be exported, transferred, destroyed, or retained for a further review at a later date).

Note: This term has a different meaning in the document management environment, where it describes a stage within the document production cycle.

role – see access control list, protective marking and security category

The level of functional (and some access), permissions granted to pre-defined subsets of users within the ERMS can be defined by use of a role.

For example, the records manager role has permissions to access many, but not all, administration functions and most record creation and access functions; the role is associated with all users who have records manager tasks.

A role definition may also include protective markings and one level of security category.

security category – see classification [2], protective marking and role

A security category can be used as a means of controlling access to fileplan objects.

Within the scope of these requirements, a security category is a form of protective marking that relates to a hierarchical series of security terms that can be applied to a fileplan object. The hierarchy should be a logical format that is clear and uses a controlled vocabulary such as that used by central government offices:

- Top Secret
- Secret
- Restricted
- Confidential
- Unclassified (default - lowest level)

Note: See the separate descriptions of protective markings in the Access Control Model on page 60for further definition.

sub-element – see element, metadata and refinement

Sub-element is a metadata attribute applied to certain records management entities, roughly equivalent to "refinement" in the e-GMS.

In a records management scheme most of the elements are applied to objects at the sub-element level (e.g. the sub-elements of **6. Date** include "**Date.Declared**", "**Date.Opened**" and "**Date.Closed**".)

superseded

A record may be superseded at any time for a variety of reasons including when guidance or procedures have been updated or when a later and more complete extract of an original record exists.

In a manner mirroring the paper record environment, the ERMS should be able to mark a record as superseded and identify a new or existing record as the superseding and definitive record.

The use of separate records for each new version ensures that version control is entirely flexible and immediately transparent. For example, each record can be stored in different areas of the fileplan, different access controls and disposal rules can be applied, etc.

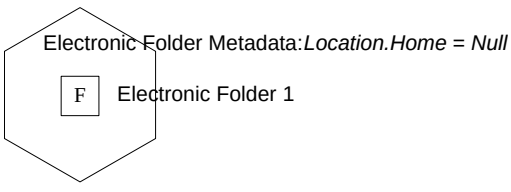
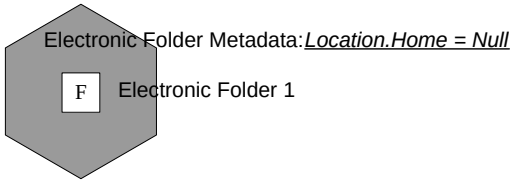
transfer – see destroy, disposal schedule, export and metadata stub

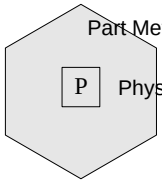
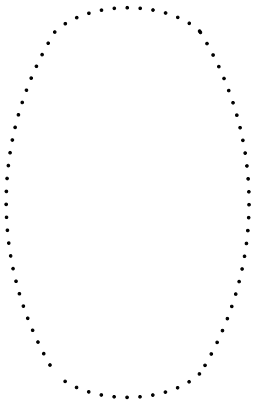
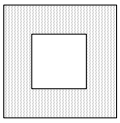
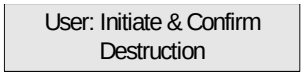
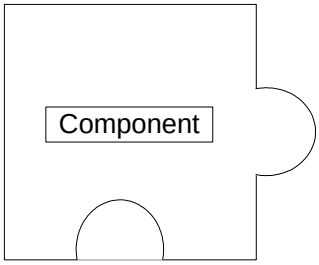
Transfer is a managed two-stage disposal action for the transfer of custody of objects in an ERMS. The transferred data may be held in a different area of an organisation or sent to archival storage for permanent preservation (e.g. The National Archives), etc.

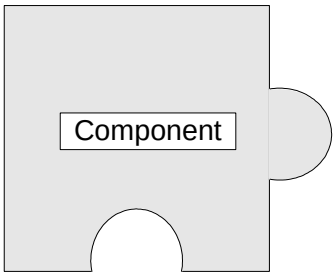
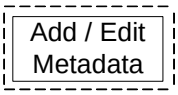
The first stage is an export disposal action. Export is used to pass copies of fileplan object metadata and content (as applicable) from one ERMS to another specified destination. The export action does not remove the exported objects from the source ERMS, and should be a repeatable process.

Once the exported data has been successfully received, verified and confirmed, the second stage of the process is a destroy disposal action to completely remove the objects from the source ERMS.

KEY FOR FIGURES

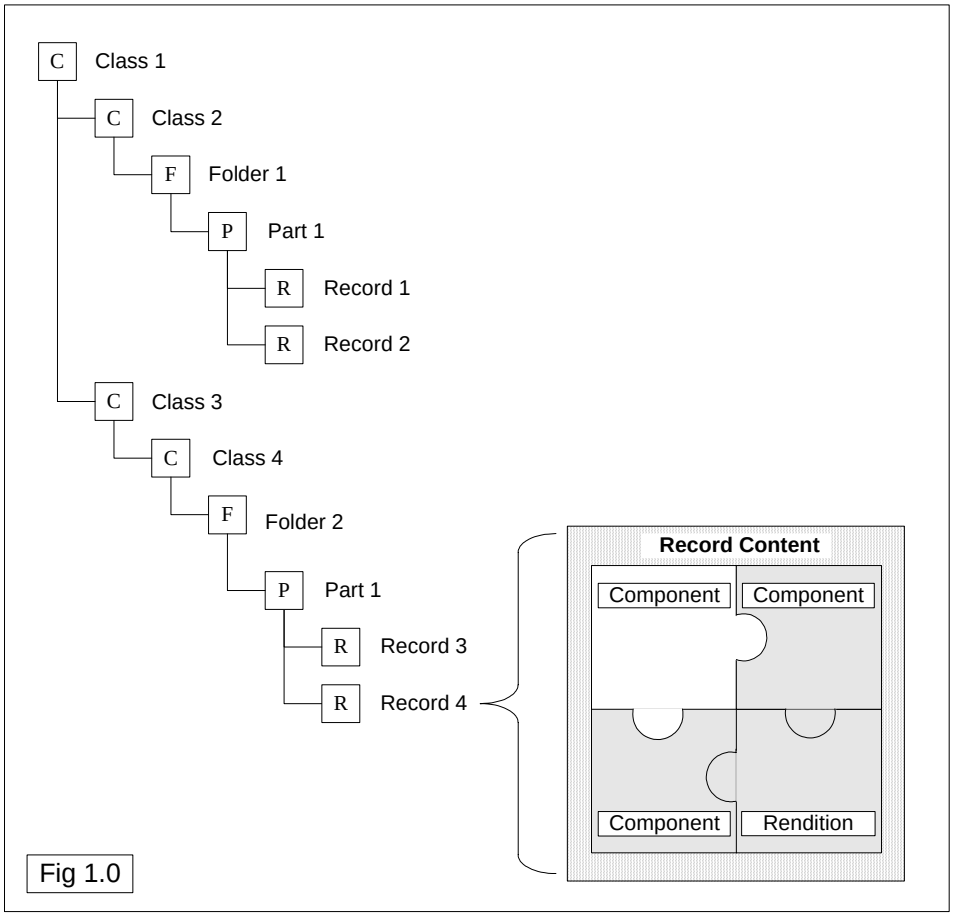
Object	Explanation
C	This represents a class within a fileplan hierarchy.
F	This represents an electronic folder within a fileplan hierarchy.
F	This represents a physical folder within a fileplan hierarchy.
F	This represents a hybrid folder within a fileplan hierarchy.
P	This represents an electronic part within a fileplan hierarchy.
P	This represents a physical part within a fileplan hierarchy.
P	This represents a hybrid part within a fileplan hierarchy.
R	This represents an electronic record within a fileplan hierarchy.
M	This represents a marker for a physical record within the fileplan hierarchy.
X	A black cross indicates where a fileplan object must not be located within a hierarchy based on standard rules and principles.
The metadata environment for each fileplan object is represented by a hexagon surrounding the object square. Individual metadata elements and their values are shown in italics.	
	Where it is important to see metadata values but there is no allocation or inheritance issue being raised, the hexagon is clear.
	Where a metadata value has been specifically allocated to the object, the hexagon is dark shaded. The metadata value is also underlined.

Object	Explanation
	Where a metadata value has been inherited by the fileplan object from its parent, the hexagon has light shading.
	The "keg" shape is used to emphasise the closely bound nature of the objects within it.
	A stippled border has been added to represent the limit of an object where the figure illustrates functionality internal and external to the object.
	A half shaded box indicates where an ERMS should be able to create an instance of the named object, or an alternative indicated where indicated. See figure 1.5 on page 33.
	A light shaded box represents an optional action or function.
	A clear jigsaw piece represents a mandatory component of a standard electronic record content.

Object	Explanation
	A light shaded jigsaw piece represents an optional component of a standard electronic record content.
	A dashed line around a text box represents an auditable event within the ERMS.
	A clear character represents any user of an ERMS. The clear character indicates that any user may perform the specified action.
	A light shaded character represents an authorised user of an ERMS. The shaded character indicates that only a suitably authorised user may perform the specified action.
	The clear and light shaded characters combined represent a range of ERMS users. The combined characters indicate that any user may perform the specified action up to a certain level, and thereafter only a suitably authorised user may perform the action.

ENTITY RELATIONSHIPS

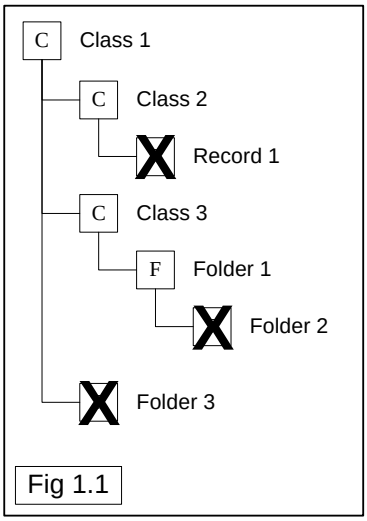
ACCEPTABLE ENTITY RELATIONSHIPS



This figure illustrates two acceptable hierarchy branches in which fileplan objects can be related to one another according to the Requirements for Electronic Records Management systems 2002. Folders are segmented by part. "Record 4" in this figure shows the potential content for a standard electronic record. See figure 1.5 on page 33 for more detail.

See key for figures on page 23.

UNACCEPTABLE ENTITY RELATIONSHIPS



This figure illustrates three unacceptable positions of objects in a fileplan. The objects that have been crossed out are unacceptable because:

- A record may not exist as the child of a class; records can only be located in folders.
- A folder may not exist as the child of a folder; folders can only be the child object of a class.
- A folder may not exist at the same level of aggregation as a class.

See key for figures on page 23.

PARENT AND CHILD FILEPLAN OBJECT RELATIONSHIPS

Parent Object Type / Child Object Type	*(Electronic) Class*	*Electronic Folder*	*Hybrid Folder*	*Physical Folder*	*Electronic Part*	*Hybrid Part*	*Physical Part*
(Electronic) Class	Yes [a]	No	No	No	No	No	No
Electronic Folder	Yes [a]	No	No	No	No	No	No
Hybrid Folder	Yes [a]	No	No	No	No	No	No
Physical Folder	Yes [a]	No	No	No	No	No	No
Electronic Part	No	Yes	No	No	No	No	No
Hybrid Part	No	No	Yes	No	No	No	No
Physical Part	No	No	No	Yes	No	No	No
(Electronic) Record	No	Yes [b]	Yes [b] [c]	No [b] [c]	Yes [b]	Yes [b] [c]	No [b] [c]
Marker (representing a physical record)	No	Yes [b] [c]	Yes [b] [c]	No [b] [c]	Yes [b] [c]	Yes [b] [c]	No [b] [c]

This table provides detail for acceptable and unacceptable child and parent fileplan object relationships within a fileplan hierarchy. Each parent object is listed across the top of the table, with acceptable child objects listed to the left.

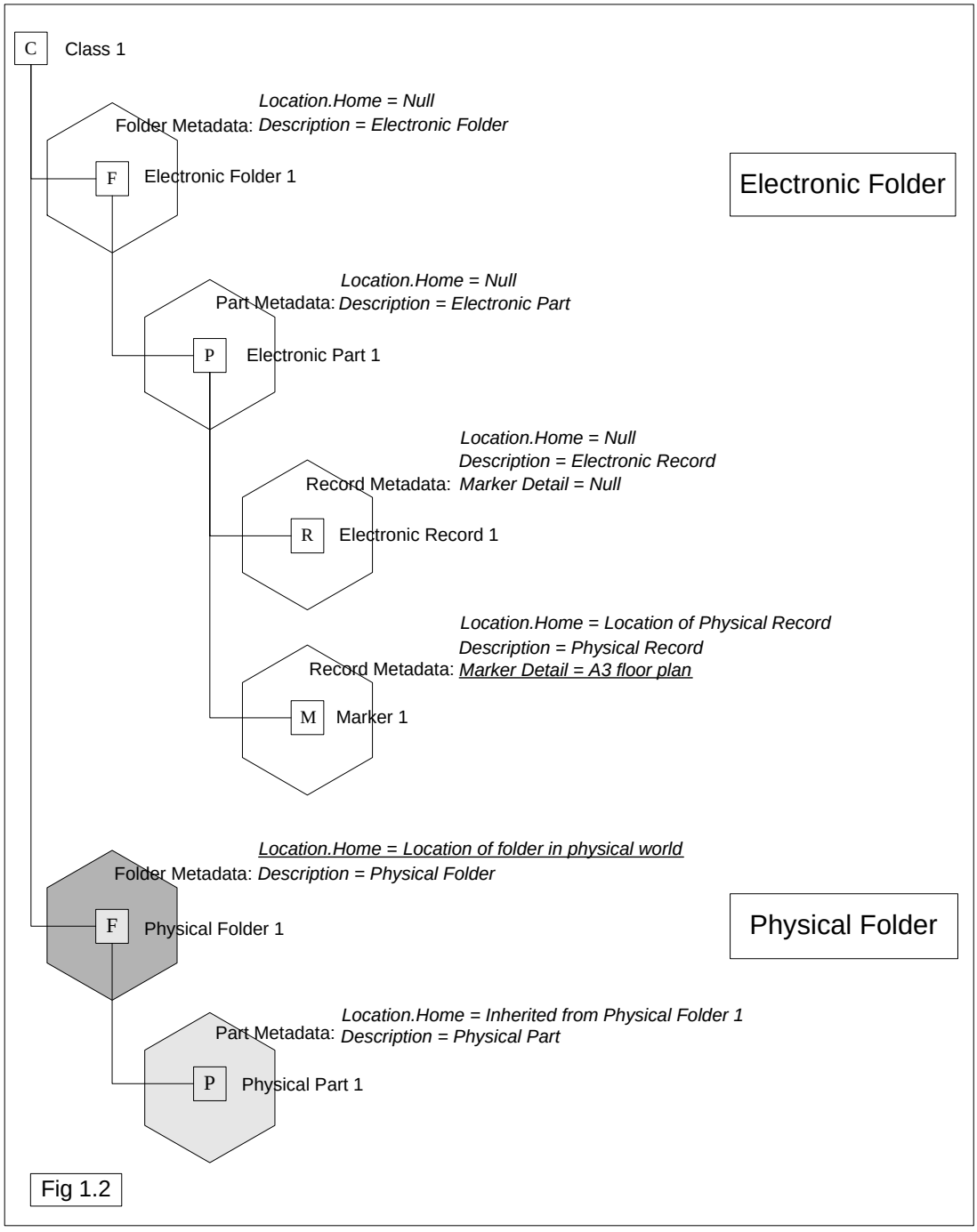
Notes

[a] The child objects associated with a class will either be a lower level class OR a folder. Classes and folders cannot exist at the same level of a hierarchical branch.

[b] Strictly speaking, records are contained within a segmented part, although an ERMS interface may present records as though they were contained directly within a folder.

[c] Within the scope of the 2002 requirements, records and markers are only expected within independent electronic folders or in the electronic aspect of a hybrid folder - i.e. physical parts are the lowest level of the physical hierarchy.

RELATIONSHIP BETWEEN AN UNRELATED ELECTRONIC AND PHYSICAL FOLDER



This figure illustrates unrelated electronic folder and physical folders; where a physical folder stands on its own, and has no relationship with an electronic folder, other than being allocated in the same class.

The physical folder metadata hexagon is shaded to indicate that the "Location.Home Location" value has been specifically allocated. Part 1 of the physical folder is more lightly shaded to show that the part inherited the location value. See key for figures on page 23.

Note: the metadata element **Marker Detail** is a custom metadata field used to help illustrate the difference between markers and electronic records. It is not part of the metadata standard

UNDERLYING HYBRID FOLDER RELATIONSHIP

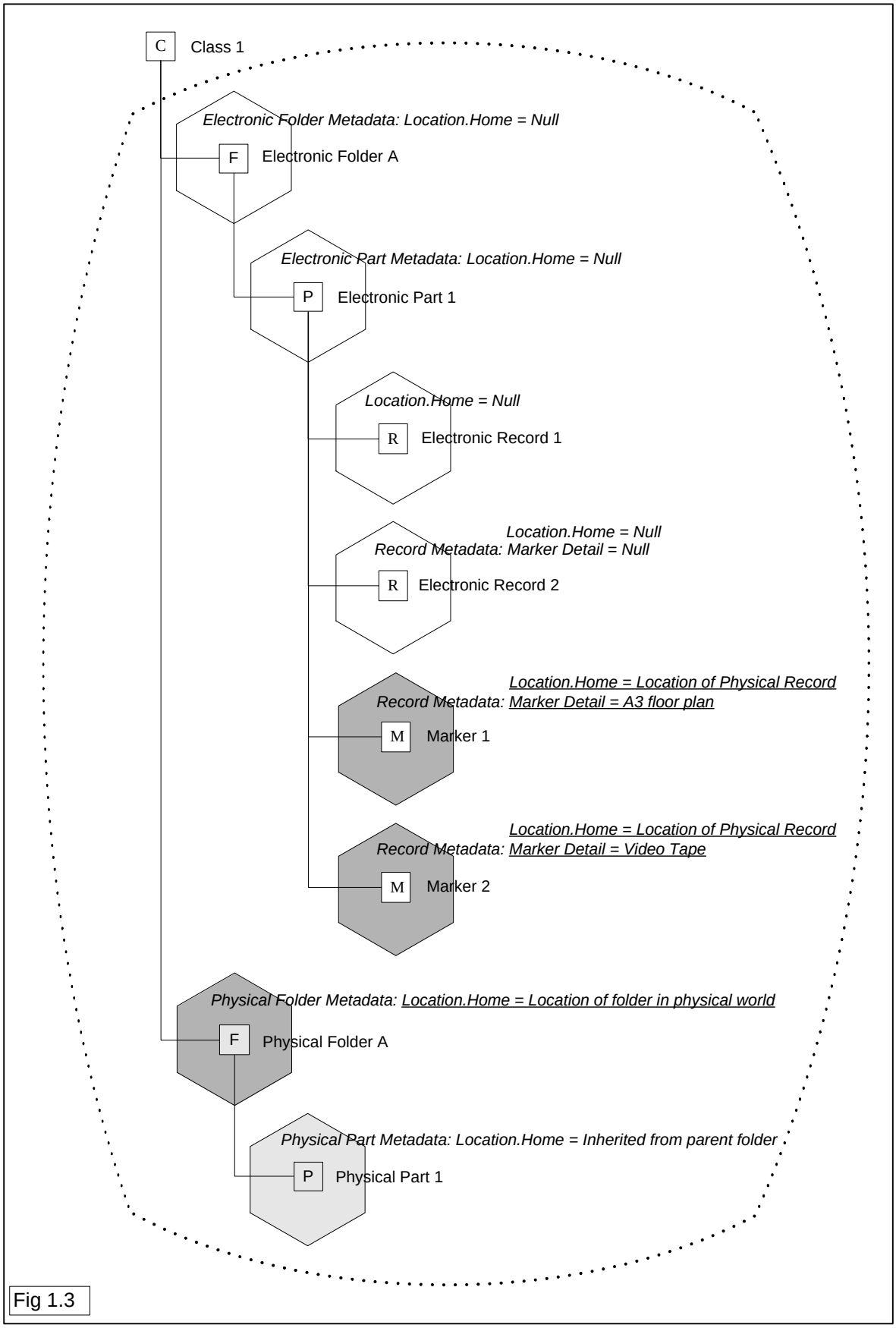


Fig 1.3

Hybrid folders allow related electronic and physical folders to be managed as a single object within the ERMS environment. The electronic and physical aspects of the folder share the same title and overall hierarchical structure.

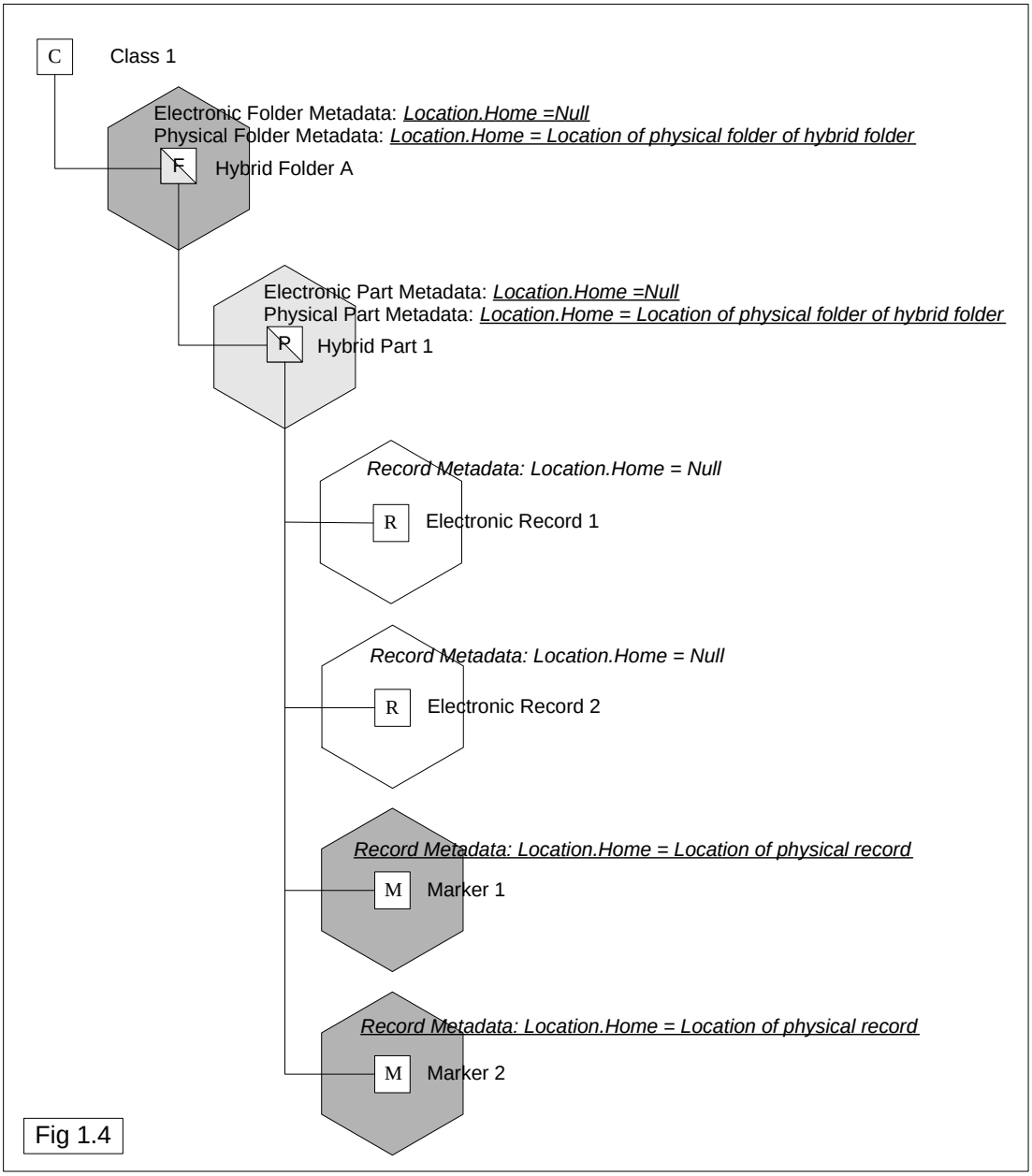
Figure 1.3 on page 30 illustrates the underlying hierarchy of a hybrid folder, with the electronic and physical aspects of the hybrid folder split out into to show the structural breakdown of all the objects. The dotted keg shape surrounding the folders is used to signify that both these folders must be managed as a single hybrid folder by the ERMS.

Note: the metadata element **Marker Detail** is a custom metadata field used to help illustrate the difference between markers and electronic records. It is not part of the metadata standard

The physical folder metadata hexagon is shaded to indicate that the "Location.Home Location" value has been specifically allocated. Part 1 of the physical folder is more lightly shaded to show that the part inherited the location value. See key for figures on page 23.

The display of the hybrid folder may vary from ERMS to ERMS. Some ERMS may display both physical and electronic objects in the same view; others may alternate between the display of electronic and physical folders (in much the same way as the different aspects were broken down in this example), providing a method to toggle between them. There are many acceptable ways of displaying hybrid folders, but all must still adhere to the conventional entity relationships as displayed in figure1.0 on page 26.

HYBRID FOLDER RELATIONSHIP



This figure illustrates a standard representation of a hybrid folder, with all electronic and physical aspects of the hybrid folder displayed as one. The hybrid folder is shaded to indicate the assignment of a value for "Location.Home Location" to the physical aspect of the folder. The hybrid part is more lightly shaded to indicate that the physical part has inherited that value. The markers are shaded to indicate their own separate "Location.Home Location" allocations.

See key for figures on page 23.

RECORD RELATIONSHIPS

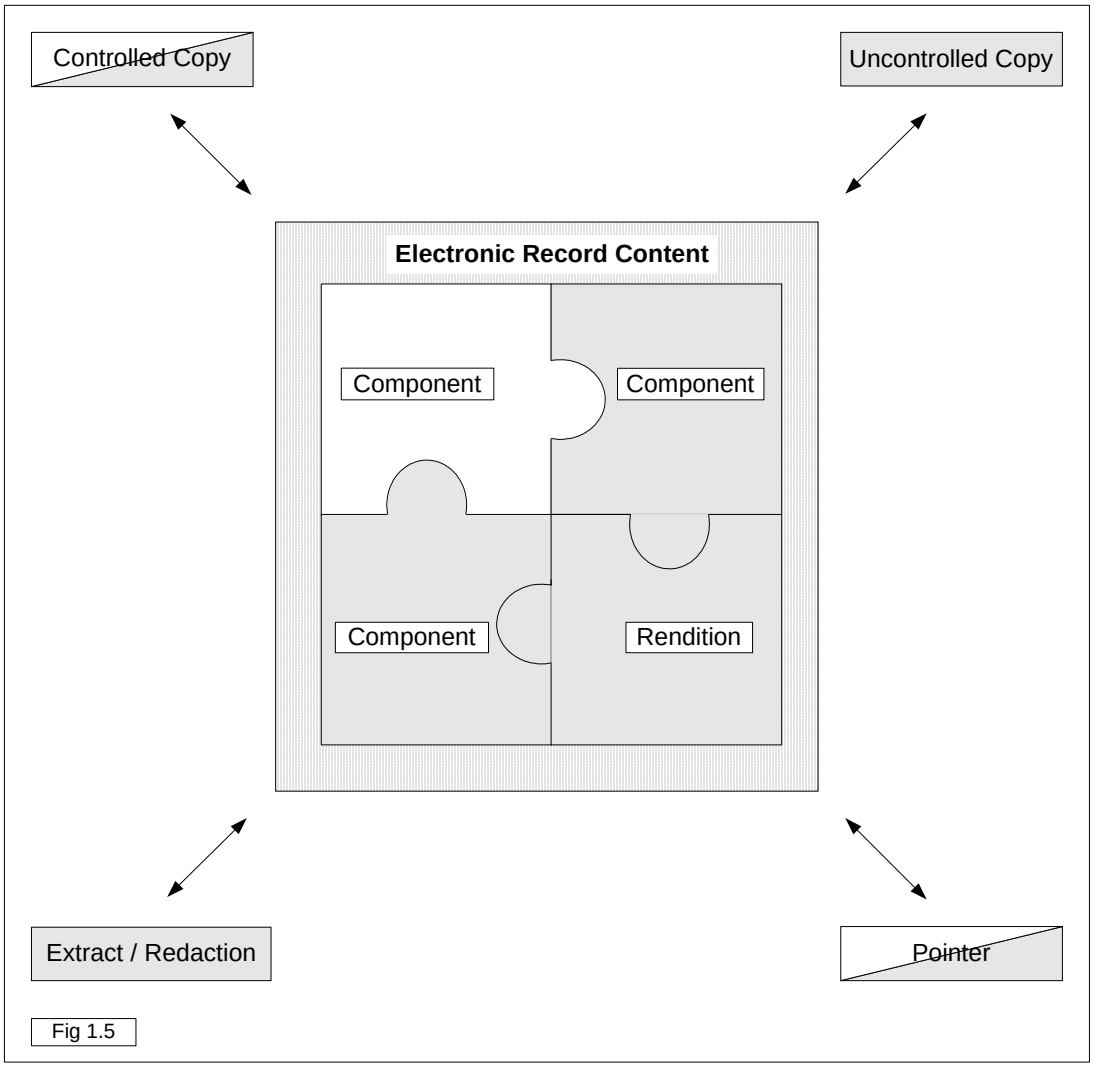


Fig 1.5

This figure shows potential content for a standard electronic record. The content of a record will always have at least one component but the number should not be limited. All record components will be tightly bound together.

Whilst this figure shows the rendition to be bound to the originating record, it must also possible to create and store a rendition as a separate record elsewhere in the ERMS (preferably including a cross-reference link between the two records).

The four corners of the figure indicate four potential related records that may exist within the ERMS environment "Pointer" and "Controlled Copy" have been half shaded to indicate that an ERMS must be able to create at least one of these instances but need not support both. "Extract / Redaction" and "Uncontrolled Copy" are fully shaded to indicate that the ability to create these instances is optional.

The double-headed arrows indicate that there must be a link from the originating record to the other instances; ideally these relational links should be two-way cross-references.

See key for figures on page 23.

DESCRIPTION OF ENTITIES

The following descriptions have been placed, where practical, into their hierarchical order to give each object their correct context and more closely relate them, in the readers mind, to the figures in the Entity Relationships section on page 26.

Note: These descriptions are an extension to the glossary entries for each entity.

Class

A class is a subdivision of an overall classification scheme by which a fileplan is organised. No assumptions are made about the principles of division, which might be based on functions, activities and subjects, or themes and sub-themes.

It is required that the classification scheme can be represented hierarchically, so that a class may relate to (be divided into) one or more classes or folders; but it can never contain records. Figure 1.0 and figure 1.1 (on pages 26 and 27 respectively) illustrate the acceptable and unacceptable methods of relating a class to other fileplan objects. A hierarchical fileplan is the way the majority of organisations continue to organise their records. A hierarchical classification must be possible, but is not mandated in implementation.

Folder

A folder is a container for related records with associated metadata attributes. Folders are created in, or allocated to, a class. See figure 1.0 on page 26. There may be many folders within a single class. A folder is the primary unit of management, and is segmented by one or more parts. Folders may not contain a class or another folder. See figure 1.1 on page 27.

In the Requirements for Electronic Records Management systems 2002 a folder is the primary unit of records management within an ERMS. Some of the folder metadata may be inherited from the class to which the folder belongs; and some may be inherited by the records, which the folder itself contains.

Regardless of their nature (i.e. electronic, physical or hybrid), every folder in the ERMS classification scheme hierarchy must be managed according to standard records management rules and principles throughout. The management of a hybrid folder and a physical folder is encompassed in anticipation of an organisation having to also manage its physical folders in the same, consistent, manner as their electronic folders.

Hybrid Folder

Hybrid folders allow related electronic and physical folders to be managed as a single object within the ERMS environment. The electronic and physical aspects of the folder share the same title and overall hierarchical structure. A hybrid folder may have one or more hybrid parts. Both the electronic and non-electronic objects of the hybrid folder must be managed as one. See figure 1.3 and figure 1.4 on pages 30 and 32 respectively.

While some metadata may differ between the electronic and physical aspects of a hybrid folder (such as the location metadata for the physical aspect of the folder), it is imperative that the ERMS ensures that specified metadata is always the same for both profiles - e.g. access controls and disposal settings must always match.

It is vital that the hierarchical structure for both environments of a hybrid folder is the same - i.e. the electronic and physical folders must be segmented into the same number of parts. If the structure was not the same, it would be impossible to exercise the proper management of the data.

The display of the hybrid folder may vary from ERMS to ERMS. Some ERMS may display both physical and electronic objects in the same view; others may alternate between the display of electronic and physical folders (in much the same way as the different aspects were broken down in this example), providing a method to toggle between them.

Note: Within the scope of these requirements, markers (which represent physical records) are only expected to be assigned to electronic folders (either standard electronic folders or to the electronic aspect of hybrid folders). It is not envisaged that markers will be assigned to physical folders in the ERMS environment.

Physical Folder

In the ERMS environment, a physical folder is a metadata profile, which represents a physical, non-electronic folder held outside of the ERMS. Typically the metadata will include the same information as for any other folder, but in addition there should also be detail about the format and location of the physical folder.

There are two scenarios where a physical folder may be represented within an ERMS:

- where the physical folder stands on its own, and has no relationship with an electronic folder in the ERMS, other than being allocated to the same classification level. See figure 1.2 on page 29.
- where the physical folder is directly related to an electronic folder in the ERMS, and shares the same title; the physical and electronic folder together constitute a hybrid folder. See figure 1.3 and figure 1.4 on pages 30 and 32 respectively.

A Physical folder may be segmented by one or more physical parts.

Note: Whilst the capture of the contents of a physical folder is not within the scope of the Requirements for Electronic Records Management systems 2002, if an ERMS permits the entry of physical records into a physical folder it is expected that markers would be used for this purpose.

Part

A part is a segment of a folder; it has no existence independent of its parent folder. A folder will always contain at least one part, the first part, and, unless a second part is created, it is co-extensive with the whole folder. Parts allow the contents of folders to be grouped and disposed of in a regular and orderly manner without need for closing the whole folder. In general the management of parts (i.e. closure, disposal, allocation of access controls) will be managed at the parent folder level.

Figure 1.0 (on page 26) shows the location of parts in the hierarchy of a fileplan. A second part may be created upon closure of the first part (and so on), allowing an organisation to effectively delineate between current and older work. The distinction between open and closed parts will remain important for the correct management of disposal. Under normal operating conditions, only the most recent part will be open at any given time.

In practice, a typical user may not always view or interact directly with parts - especially where only one part exists - as the ERMS will by default place records automatically into the most recent open part. For management purposes, the ERMS must be able to display parts within the full fileplan hierarchy to an authorised user.

Note: strictly speaking, records are contained within a segmented part, although an ERMS interface may present records as though they were contained directly within a folder.

Hybrid Part

A hybrid part is a segment of a hybrid folder; it has no existence independent of its parent hybrid folder. The hybrid part may contain one or more electronic records and markers for physical records. Electronic and physical objects must be managed in the same way by the ERMS. A hybrid part should be managed as a single logical entity, including metadata values for elements such as **Location.Home Location** which it will inherit from its parent hybrid folder, figure 1.3 and figure 1.4 on pages 30 and 32.

An ERMS must ensure that the electronic and physical parts are co-ordinated as one; for example, the electronic part 1 of a hybrid folder is always associated with the physical part 1, and both have the same open and close dates.

In practice, a typical user may not always view or interact directly with a hybrid part - especially where only one part exists - as the ERMS will by default place records automatically into the most recent open part. For management purposes, the ERMS must be able to display all hybrid parts within the full fileplan hierarchy to an authorised user.

Note: Records are sometimes considered as held within a folder, but more properly are stored in a segmentation of the folder, i.e. a part.

Physical Part

A physical part is a segment of a physical folder; it has no existence independent of its parent folder. The physical part cannot contain any records in the model used for the Requirements for Electronic Records Management systems 2002. A physical part must be managed as a single logical entity, including metadata values for elements such as **Location.Home Location** which it will inherit from its parent physical folder, see figure 1.2 on page 29.

In practice, a typical user may not always view or interact directly with a physical part - especially where only one part exists - as the ERMS will by default place records automatically into the most recent open part. For management purposes, the ERMS must be able to display all physical parts within the full fileplan hierarchy to an authorised user.

Note: Records are sometimes considered as held within a folder, but more properly are stored in a segmentation of the folder, i.e. a part.

Record

A standard electronic record is consists of both content (i.e. one or more components) and metadata. It may be a single component, such as a word processed document, or spreadsheet. It could also be a set of closely bound components that are meaningfully treated as one object, such as a web page or multimedia document see figure 1.5 on page 33.

Records are contained in folders, and segmented by part. They can never be contained in a class or outside of the fileplan hierarchy (orphaned). A record may inherit some of its metadata from the folder to which it is assigned, for example in relation to disposal and access controls.

Whilst documents can be edited and deleted, electronic records are held in a fixed state with appropriate access and functional permissions applied.

Physical record

A Physical record is a record that exists outside of an ERMS in a non-electronic environment. It may be held as paper, microform, magnetic, or any other physical medium. A metadata profile (i.e. marker) is can be used to represent physical records within an ERMS environment.

Similar to an electronic record, a physical record (as a marker) will have metadata populated for it within an ERMS. Whilst documents can be edited and deleted, electronic records are held in a fixed state with appropriate access and functional permissions applied. See figure 1.3 and figure 1.4 on pages 30 and 32 respectively.

Note: Whilst the listing of the contents of a physical folder is not within the scope of the Requirements for Electronic Records Management systems 2002, if an ERMS permits the entry of records into a physical folder, it is expected that markers would be used for this purpose.

Marker (for a physical record)

A marker is an electronic metadata profile which can be used to represent physical records within an ERMS environment in a similar manner to standard electronic records. Markers are used to denote a physical object that cannot be entered into an ERMS because it is either a physical object (i.e. paper or video) or because it is not suitable to be stored in an ERMS (i.e. a large database).

Unlike an electronic record, markers have no electronic content.

Markers may be captured as a default record_type record with the addition of a value in the location metadata field. Where this is the case a ERMS may provide a different icon for a marker in than for a standard electronic record. Alternatively, a marker may be defined as a fileplan object in its own right, completely independent of electronic records. It may then be possible to create metadata profiles for markers, which define the characteristics for different kinds of marker objects in a similar manner to record_types.

Due to the nature of markers their "Location" metadata elements must be populated. Figure 1.2 and figure 1.3 (on pages 29 and 30 respectively) provide an example of how **Location.Home Location** metadata differentiates a marker from a standard electronic record within the ERMS.

Within the scope of these of the Requirements for Electronic Records Management systems 2002 markers are only expected to be placed in an electronic folder be it an electronic folder on its own or part of a hybrid folder.

Note: Whilst not originally envisaged by the model of the Requirements for Electronic Records Management systems 2002, many ERMS will allow the use of markers for listing the contents of physical folders within an ERMS.

Extract (Redaction)

An extract is a copy of a record, from which some material may have been removed or permanently masked (redacted). An extract is often made when the full record cannot be released, for example under the Freedom of Information Act 2000, but part of the record can.

While some records may never require the creation of an extract, other records may have several different extracts where content may vary depending on the sensitivity of the material.

In general it is expected that an extract would be declared as a separate record within the ERMS hierarchy, typically in a different folder to the originating record. See figure 1.5 on page 33

Note: some advanced systems may allow extract components to be tightly bound within the originating record. The ERMS functionality would manage the whole record in an appropriate manner, applying strict access controls and viewing functionality to ensure that users only have access to the appropriate aspects of the record.

Component

A component is the smallest aggregation of data managed by an operating system. A record may be comprised of one or more components. An example of typical single component record content is a single, stand-alone spreadsheet. An example of multi-component record content is a webpage that is comprised of HTML and separate image components.

Typical end users will not be able to interact directly with the individual components - i.e. users would normally engage with the content from the document or record level.

Whilst a typical end-user may be able to interact with a component, they will only ever be able to perform the interaction via the record itself. For example where an email record has been stored with its attachments as one record, the attachment components will not be visible within the fileplan, or by any other means other than opening the email record.

Components must be properly maintained by an ERMS so that associated properties are recorded and managed as required over time, e.g. for migration purposes. Components must be retrievable and displayed in the same manner as observed in their original format. Figure 1.5 (on page 33) illustrates the relationship of a standard electronic record to its components and other instances of the record that may be created.

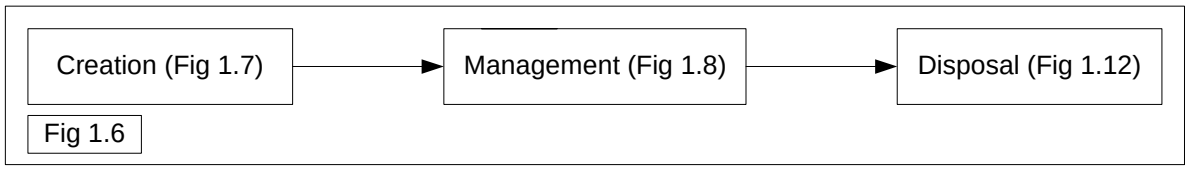
Additionally components do not represent another level of aggregation within the ERMS they are shown here for completeness, but the Requirements for Electronic Records Management systems 2002 and accompanying metadata model do not address component management beyond initial recognition. The National Archives have developed a series of publications providing requirements for sustainability, and can be found on the website: Requirements to sustain electronic information over time

Note: the term "component" has been defined as such for the Requirements for Electronic Records Management systems 2002; it is not in widespread use elsewhere.

ENTITY LIFE HISTORIES

FOLDER ENTITY LIFE HISTORY

This section presents the entity life history of an electronic folder. The entity life history figures show the management of a folder from initial creation, management (including the addition of records to one or more parts), to its eventual destruction or permanent preservation in an archive as a complete folder with all the records that it contains.



This figure provides a brief outline of 3 key stages in a folder's lifecycle.

FOLDER CREATION

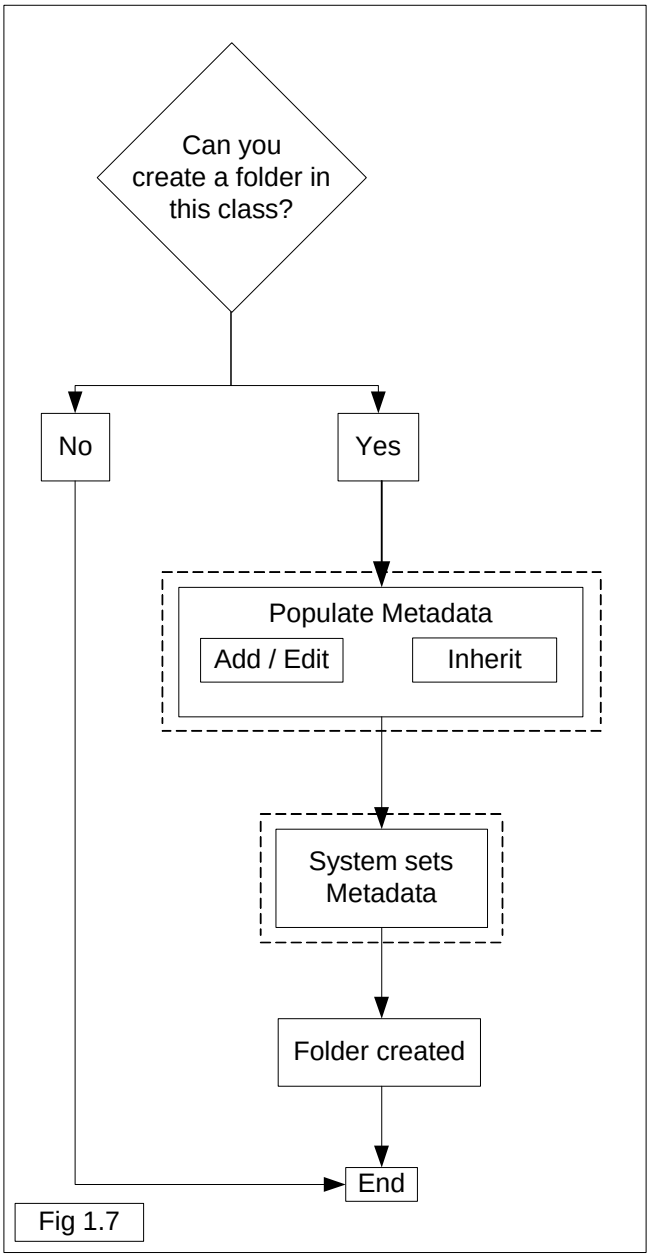


Fig 1.7

Only authorised users will be able to create folders. As part of this process, metadata (both ERMS generated and user-defined) will be populated as appropriate. The ERMS saves the metadata values and the folder creation process is complete.

The dashed boxes indicate where audit events are automatically recorded by the ERMS.

See key for figures on page 23.

FOLDER MANAGEMENT

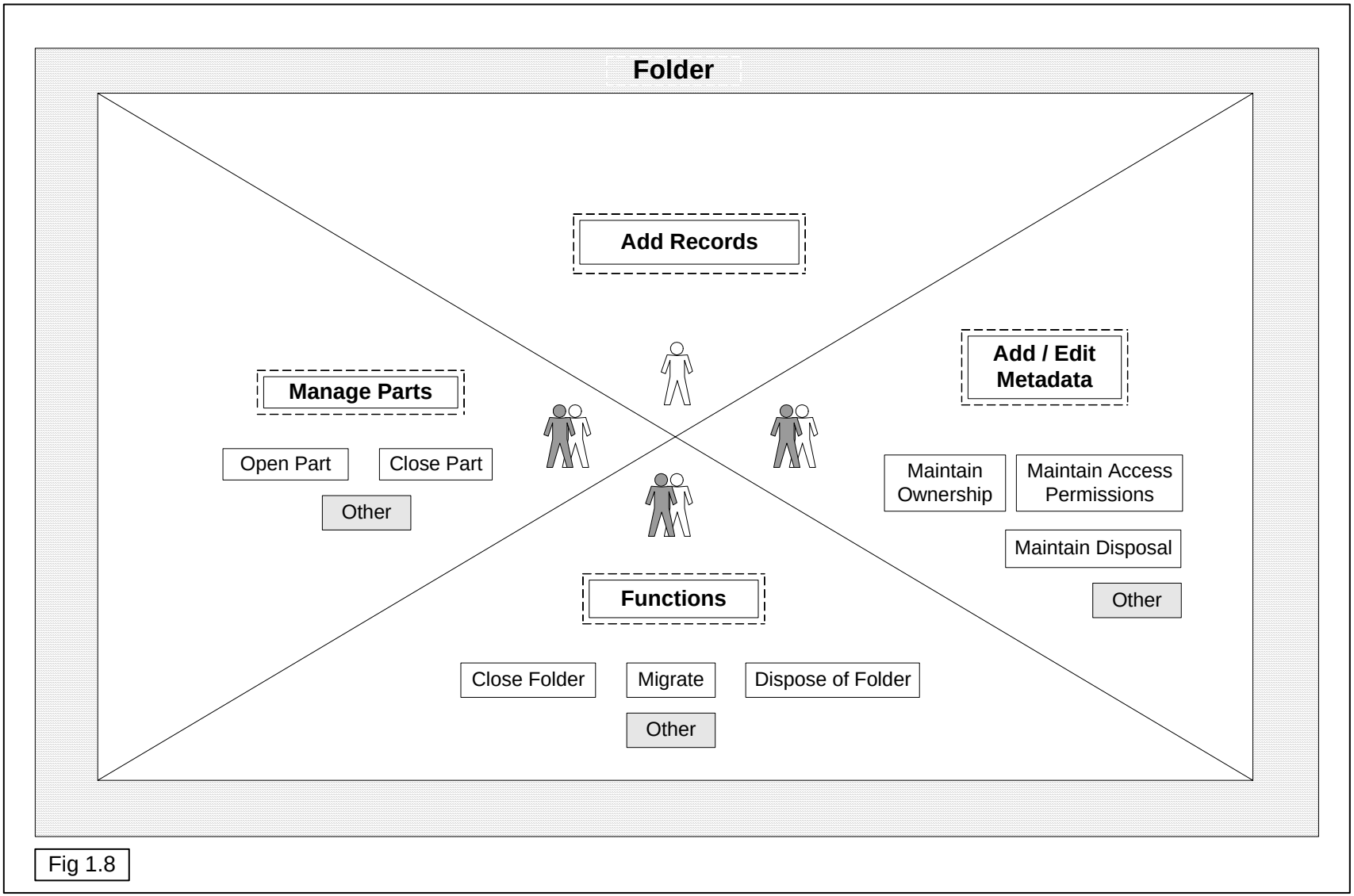


Fig 1.8

This figure illustrates key functions and activities that may be performed on a folder, by different users, during its life within an ERMS. Every folder within an ERMS must be properly managed - even a closed folder must be managed until it is removed from an ERMS.

The examples of each management activity are for illustrative purposes and are not an exhaustive list of every aspect of folder management. The main functions are highlighted in bold text, with specific, related functions grouped together in each segment of the "envelope".

The dashed boxes indicate where audit events are automatically recorded by the ERMS. Auditable events may be configured differently from ERMS to ERMS but the diagram highlights the key areas that would normally be monitored.

The clear characters indicate any user can perform that folder management activity. Shaded characters indicate only an authorised user can manage that activity. Where both appear together, for example "Add / Edit Metadata", all users will be able to carry out a certain number or level of functions, while only authorised users will be able to perform higher level (often administrative) folder management functions.

See key for figures on page 23.

FOLDER DISPOSAL

As part of their lifecycle all fileplan objects may be disposed of. Each disposal action must be performed in a well-managed and controlled way within the ERMS environment.

The ERMS must ensure prevent the destruction or deletion of an electronic folder and any of its records and metadata at all times, with the exceptions of:

- destruction in accordance with a disposal schedule (A.4.67)
- deletion by an Administrator as part of an audited procedure (A.4.65)[9]

Figure 1.12 on page 57 explores the generic disposal management process for any fileplan object within an ERMS.

[9] *Functional Requirement A.1.46M, Requirements for Electronic Records Management Systems 2002*

COMMENTARY: FOLDERS

KEY CONCEPTS

- A record is, by default, governed by the folder with which it is associated for purposes of management and disposal[10]. See Commentary: Records on page 54.
- By default, complete folders of records are managed and disposed of as a whole without selective removal of parts or records[10].
- Folders must be properly managed over time, even after closure.
- Access controls may be applied separately to folders and non-default specific record_type records within each folder. Access controls can only be applied to a folder by a suitably authorised user. See Access Control Model on page 60.

LIFE HISTORY EVENTS

Events in figure 1.7, figure 1.8, and figure 1.12 (on pages 41, 42 and 57 respectively)are briefly described in this section. The actions have been listed in alphabetical order. It should be noted that the commentary entries provided here relate to the examples provided and are not exhaustive. In addition to specific events, some entries provide generic details for a main event identified in one or more of the example diagrams.

Add / Edit folder metadata – see figure. 1.8 on page 42

Metadata that is not ERMS generated and controlled can be added or edited by a suitably authorised user upon creation, or it may have to be completed after the creation process. Some metadata must remain editable by an authorised user throughout a folder's existence within an ERMS.

Disposal and access controls have been separated here as examples of metadata elements that will be populated and managed during the folder lifetime.

Add records – see figure. 1.8 on page 42

An electronic record is added to the folder directly by the user as it is declared in normal business operations.

Upon capture / declaration a record, or marker, will be managed by default at the folder level. This includes (but is not limited to) metadata for access controls and disposal. Capture / declaration of records is discussed in more detail in the Commentary: Records chapter on page 54.

Under normal operating circumstances, it is expected that all users will be able to add records.

[10] *The only permissible exception to this is where a specific record_type has been defined and implemented in the ERMS (e.g. Functional Requirement A4.31M, Requirements for Electronic Record Management systems.*

Allocate disposal schedule – see figure. 1.12 on page 57

Only an authorised user will be able to allocate a disposal schedule. A disposal schedule may be allocated upon the creation of a folder, or at a later date. It must also be possible for an authorised user to change the disposal schedule at anytime.

The disposal schedule should include:

- A triggering event, such as the closure of a folder.
- A retention period, such as 6 years and 2 months.
- A disposal action, such as review, export, transfer, or destroy.

Allocate / Execute Final Disposal Schedule – see figure. 1.12 on page 57

A final disposal schedule involves a disposal action of either transfer or destroy. Upon destruction, the folder, and child objects, will be removed entirely from the ERMS.

Note: When a folder is transferred, the folder will only be removed from the ERMS **after** the second stage of the transfer action (i.e. the destroy action, and **not** the export action).

Annotate decision – see figure. 1.12 on page 57

Desirably, the reasons for a review decision to retain a folder are included with the folder metadata for use in later reviews. For example, comments may be provided for the reallocation of a review disposal schedule.

Audit trail data - see figure 1.7, figure 1.8, and figure 1.12 pages 41, 42, and 57 respectively.

The audit trail logs events that occur to the folder from its creation, throughout its lifetime within an ERMS, and eventual deletion or destruction. Examples of auditable events include folder creation, adding or moving records, opening parts, or editing the folder's metadata.

While the auditable events within a ERMS may be configurable, once activated, the ERMS audit trail must record information about specified events without manual intervention. Audit trail data for a folder must be retrievable by authorised users for scrutiny as required.

Close folder – see figure. 1.8 on page 42

The folder as a whole is closed, so that no further records can be added to any part within it.

Note: The ERMS must allow the re-opening of a folder by an authorised user for administrative purposes as required.

Close part – see figure. 1.8 on page 42

The currently open part is closed so that no further records can be added to it. If the folder as a whole is not also closed a new part may be opened. Whenever a new part is opened, the ERMS must ensure that the previous part is automatically closed.

Note: The ERMS must allow the re-opening of a part by an authorised user for administrative purposes as required.

Create folder – see figure. 1.7 on page 41

Suitably authorised users can create a folder in an appropriate class within the fileplan structure. Upon creation a folder will be allocated a meaningful title and reference code. Folder metadata will be system-generated and / or manually populated based on the standard ERMS creation process.. Once a folder has been created, it is ready to receive records.

Destroy – see figure. 1.12 on page 57

Destroy is a managed disposal action for the total removal of fileplan objects from the ERMS and underlying database. When folders are destroyed, it might be desirable to retain a metadata stub of the object as evidence of its existence.

Destruction as a managed disposal action should not be confused with deletion, which would allow suitably authorised users to remove data on an ad-hoc basis as part of a controlled and audited action.

Disposal of folder – see figure. 1.12 on page 57

Upon execution of a disposal schedule, a specified disposal action will be performed on the folder (e.g. review, transfer, or destroy). Only an authorised user may allocate and execute a folder's disposal schedule. Review and export disposal actions may occur as many times as necessary, but a final disposition (destroy or transfer) will only occur once.

Note: By default the disposal schedule will be allocated at the folder level and inherited by all parts and records contained within the folder. Upon execution, the folder and all its contents will be dealt with as one action.

Export – see figure. 1.12 on page 57

Export is a managed disposal action for passing copies of fileplan object metadata and content (as applicable) from one ERMS to another specified destination. Export is a repeatable process and may be performed as often as required. Export (as opposed to transfer) does not remove the exported objects from the source ERMS, and should be a repeatable process.

Functions – see figure. 1.8 on page 42

A folder may be subject to any number of functions during its lifetime within an ERMS fro creation to disposal. Figure 1.8 provides some examples of what these functions may be, it is not an exhaustive list of all the possible functions.

Whilst not all functions will be captured in the audit trail, some events, for example folder closure, allocation of access permissions, and disposal must be audited.

Inherit Metadata – see figure. 1.12 on page 57

Upon creation a proportion of folder metadata will, by default, be inherited from its parent class in the fileplan. All inherited metadata values (e.g. access controls) will be applied to child objects unless explicitly overridden by an authorised user or ERMS rule.

Maintain access controls – see figure. 1.8 on page 42

The access controls for a folder will be set either on creation, or shortly after. Once set only users with all the appropriate access permissions will be able to view the folder.

Access controls for a folder may be changed during its lifetime (whether open or closed). As its contents become less, or more, sensitive the folder's access controls must be changed to reflect this. See Access Control Model on page 60.

Note: An example of an access controls is Protective Marking (i.e. security category) with the value "secret".

Maintain audit data – see figure 1.7, figure 1.8, and figure 1.12 pages 41, 42, and 57 respectively

Audit data will be maintained for both open and closed folders. Once initiated, the audit trail will automatically log specified events and actions within the ERMS without any user interference.

Maintain ownership – see figure. 1.8 on page 42

Ownership of the folder may change as individuals and business unit's change. Change in ownership must be limited to suitably authorised users, with details captured by the audit trail.

Manage folder – see figure. 1.8 on page 42

Each folder must be managed throughout its lifetime, including its parts and records. A folder will also be managed after it has been closed until it is removed from the ERMS. Certain types of folder management will be limited to suitably authorised users such as the allocation of disposal schedules and access controls.

Manage parts – see figure. 1.8 on page 42

Parts may be closed, and new parts opened, until the folder is closed.

Migrate – see figure. 1.8 on page 42

Folders may need to be migrated as hardware and software platforms change, by conversion to new media and / or formats.

Open part – see figure. 1.8 on page 42

An ERMS must allow a new part to be opened within the folder. Under normal operating conditions, only one part may be open at any time within a folder.

New parts can not be opened when the folder is closed.

Note: When opening a new part the ERMS must automatically close the previous part, if not already closed.

Re-allocate disposal schedule – see figure. 1.12 on page 57

During a folder's lifetime it may be necessary to update the disposal properties to reflect business needs, etc. Disposal schedules are typically allocated following a review process, with the result that either the same disposal schedule is re-allocated or a new disposal schedule is applied.

Review – see figure. 1.12 on page 57

Review is a managed disposal action for examining the metadata (including disposal schedule status) of the folder - i.e. should it be exported, transferred, destroyed, or retained for a further review at a later date. Review is a repeatable process and may be performed as often as required.

System sets metadata – see figure 1.7 on page 41

While authorised users may be able to edit some specified metadata, there will be other metadata fields (particularly those containing system defined values) that will only ever be read-only; i.e. no user will be able to edit these values at any time. This is essential in order to maintain the integrity and authenticity of the record.

Transfer – see figure. 1.12 on page 57

Transfer is a managed two-stage disposal action for the transfer of custody the folder in an ERMS. The transferred data may be held in a different area of an organisation or sent to archival storage for permanent preservation (e.g. The National Archives), etc.

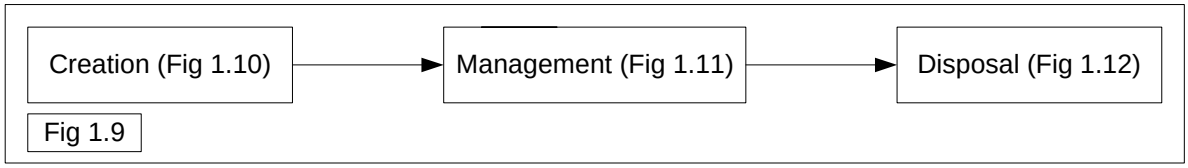
The first stage is an export disposal action. Export is used to pass copies of the folder metadata and content (as applicable) from one ERMS to another specified destination. The export action does not remove the exported folder (or its child objects) from the source ERMS, and should be a repeatable process.

Once the exported data has been successfully received, verified and confirmed, the second stage of the process is a destroy disposal action to completely remove the folder from the source ERMS.

Note: The ERMS must allow the transfer to be paused, or cancelled, prior to the destruction stage. This is to ensure that no data is lost if the exported objects are corrupted during the export stage of the process - i.e. the folder will not be destroyed until appropriate confirmation has been received regarding the export data.

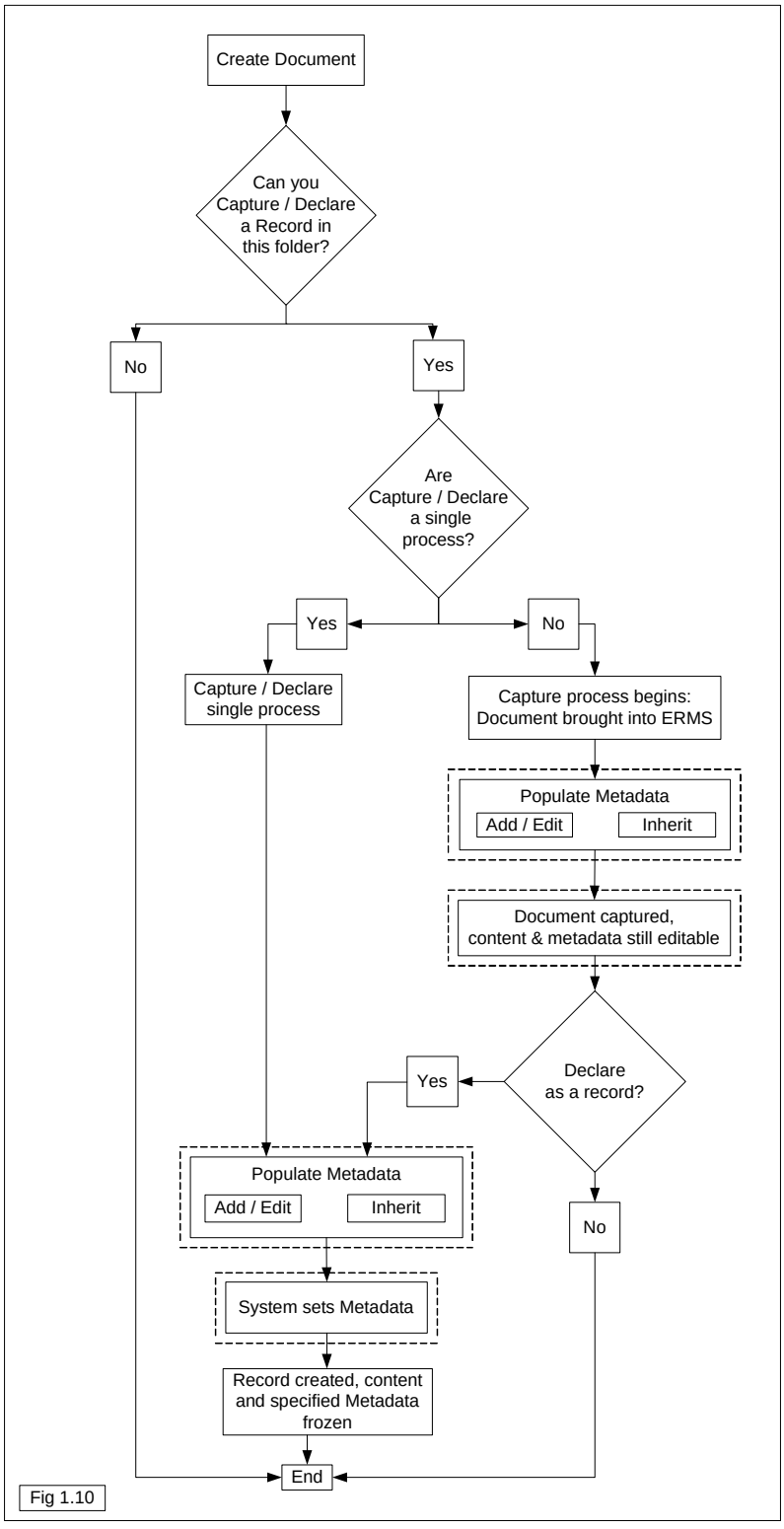
ELECTRONIC RECORD ENTITY LIFE HISTORY

This section presents the entity life history of a record. The entity life history figures show the management of a record from initial creation and management to its eventual destruction or permanent preservation in an archive.



This figure provides a brief outline of 3 key stages in a record's lifecycle.

RECORD CREATION



This figure explains how capture and declaration may be treated by different ERMS products. Metadata (both ERMS controlled and user editable) will be populated as appropriate to the ERMS' record creation mechanism.

The dashed boxes indicate where audit events are automatically recorded by the ERMS. See key for figures on page 23.

MANAGE RECORD

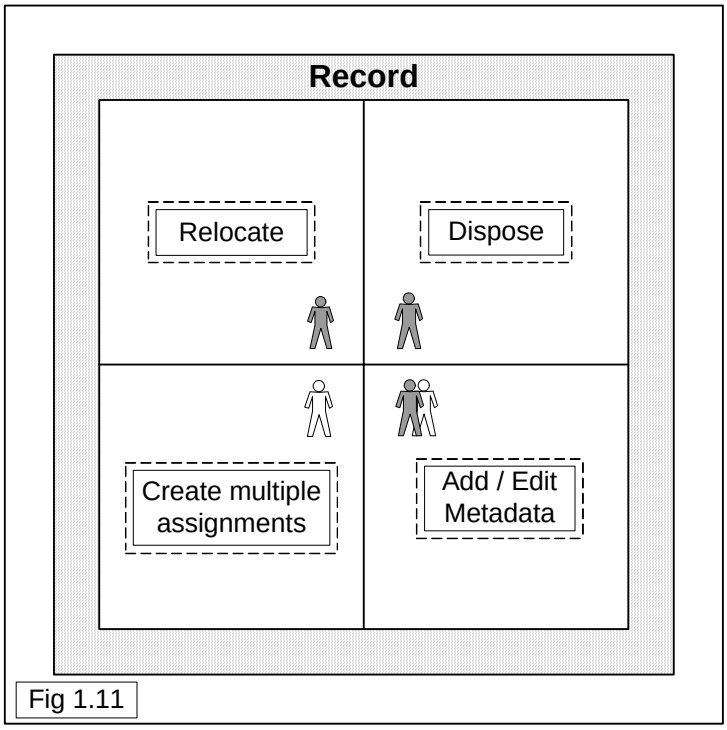


Fig 1.11

This figure illustrates key management actions that may be performed on a declared record during its life within an ERMS.

The dashed boxes indicate where audit events are automatically recorded by the ERMS. Auditable events may be configured differently from ERMS to ERMS but the diagram highlights the key areas that would normally be monitored.

The clear characters indicate any user can perform that record management activity. Shaded characters indicate only an authorised user can manage that activity. Where both appear together, for example "Add / Edit Metadata", all users will be able to carry out a certain number or level of functions, while only authorised users will be able to perform higher level (often administrative) record management functions.

See key for figures on page 23.

RECORD DISPOSAL

As part of their lifecycle all fileplan objects may be disposed of. Each disposal action must be performed in a well-managed and controlled way within the ERMS environment.

By default, records will normally be disposed of along with their parent folder or part - essentially these records will inherit the disposal properties from their parent objects. However, records of a non-default, specific record_type may be assigned a different disposal schedule, allowing those records to be disposed of using the standard disposal mechanism.

Figure 1.12 on page 57 explores the generic disposal management process for any fileplan object within an ERMS.

COMMENTARY: RECORDS

KEY CONCEPTS

- A version of a document may be declared as a record at any time.
- Upon declaration record content cannot be changed (but some metadata, e.g. access controls, can be changed).
- A record's disposal will be managed by default at the folder level. Exceptionally where a record is allocated to a non-default specific record_type definition, with a specific disposal schedule, the record's disposal will be determined by the disposal schedule for that record_type definition.

Note: Where folder and record_type disposal schedules are both applied a disposal conflict may result. The ERMS must manage and draw attention to conflicts at an appropriate time.

LIFE HISTORY EVENTS

Events in figure 1.10, figure 1.11, and figure 1.12 (on pages 51, 52 and 57 respectively) are briefly described in this section. The actions have been listed in alphabetical order. It should be noted that the commentary entries provided here relate to the examples provided and are not exhaustive. In addition to specific events, some entries provide generic details for a main event identified in one or more of the example diagrams.

Maintain Access controls

The access controls for a record will be set either on creation, or shortly after. Once set only users with all the appropriate access permissions will be able to view the record.

Access controls for a record may be changed during its lifetime. As a record becomes less, or more, sensitive the record's access controls must be changed to reflect this. See Access Control Model on page 60.

Note: An example of an access control marking is a Protective Marking (i.e. security category) with the value "secret".

Add / Edit metadata – see figure. 1.11 on page 52

Metadata that is not system generated and controlled can be added or edited by a suitably authorised user upon capture / declaration, or it may have to be completed after the record is declared.

Disposal and access controls have been separated here as examples of metadata elements that may be populated and managed during the record's lifetime.

Apply changes – see figure. 1.10 and figure. 1.11 on pages 51 and 52 respectively

When document content and / or metadata is changed (for example when applying annotations to an electronic document in the same manner as might be made to a paper record) the ERMS will create a new version of the document reflecting those changes.

Audit trail data – see figure. 1.10 and figure. 1.11 on pages 51 and 52 respectively

The audit trail logs events that occur to a record from its creation within the ERMS and throughout its lifetime to eventual export or destruction. Examples of auditable events include record declaration, moving records, creating a rendition, or editing the record's metadata.

While the auditable events within an ERMS may be configurable, once activated, the ERMS audit trail must record information about specified events without manual intervention. Audit trail data for a record must be retrievable by suitably authorised users for scrutiny as required.

Capture– see figure. 1.10 on page 51

Capture involves the placing of a document (or record) within the control of an ERMS. Where an ERMS is capable of managing both documents and records, capture and declaration are likely to be available as separate processes.

Classify – see figure. 1.10 on page 51

Classification involves the addition of a document or record to a folder within the fileplan.

Create document – see figure. 1.10 on page 51

An electronic document may be created outside of the ERMS environment using a range of applications such as word processing software or e-mail client.

Note: Physical documents may exist in a variety of formats including physical objects such as large maps, DVDs, etc.

Create multiple assignments – see figure. 1.11 on page 52

During its lifetime within an ERMS it may be necessary to assign a record to more than one location within the fileplan. Ideally this would be achieved by the use of pointers. Where pointers are not available the ERMS should offer the ability to create a controlled copy of a record (that is a copy using a specific ERMS function) that can be located in another location.

Regardless of the method used the ERMS must retain a link from the originating record to any other instances, and ideally, a link from any other instance back to the originating record.

Whenever another assignment of a record is created, the action must be properly managed and it must be logged in the ERMS audit trail.

Declare – see figure. 1.10 on page 51

A suitably authorised user can declare a document once it has been decided that the content is final.

Upon declaration the content of the record is fixed and cannot be changed. Authorised users may be able to edit specific metadata for example access controls or disposal schedule.

Disposal of records– see figure. 1.12 on page 57

Upon execution of a disposal schedule, a specified disposal action will be performed (e.g. review, export, transfer, or destroy). By default, record disposal is managed by the disposal schedule allocated to the parent folder, or part.

Where a record is of a specific non-default record_type definition its disposal will be primarily governed by any disposal schedule allocated to that record_type definition.

If a destroy action is executed it may be desirable that the ERMS retains a metadata stub of the object as evidence of its existence.

Note: Where folder and record_type disposal schedules are both applied this may result in a conflict. The ERMS must manage and draw attention to conflicts at an appropriate time.

Document – see figure. 1.10 on page 51

A document may be held electronically or in other physical media such as on paper. It may include any combination of text, data, graphics, sound, moving pictures or any other forms of information. A single document may consist of one or more components; the key aspect is that a document's content and some metadata are still editable, unlike a record.

Freeze contents– see figure. 1.10 on page 51

Upon declaration the content of the record is fixed and cannot be changed. When users view the record content, it is presented in a read-only format and edits are not permitted. Authorised users may be able to edit specific metadata for example access controls or disposal schedule. This is essential in order to maintain the integrity and authenticity of the record.

Inherit Metadata– see figure. 1.10 on page 51

A proportion of record metadata will, by default, be inherited from its parent folder in the fileplan. All inherited metadata values (e.g. access controls) will be applied to child objects unless explicitly overridden by an authorised user or system rule.

Record – see figure. 1.10 on page 51

In the Requirements for Electronic Records Management systems 2002, a record is a document that has been formally declared into an ERMS. Records can only be allocated to a folder within an ERMS (with the record held within the currently open segmented part of the folder).

System sets metadata– see figure. 1.10 on page 51

While authorised users may be able to edit some specified metadata, there will be other metadata fields (particularly those containing system values) that will only ever be read-only; i.e. no user will be able to edit these values at any time. This is essential in order to maintain the integrity and authenticity of the record.

GENERIC DISPOSAL SCHEDULE PROCESS

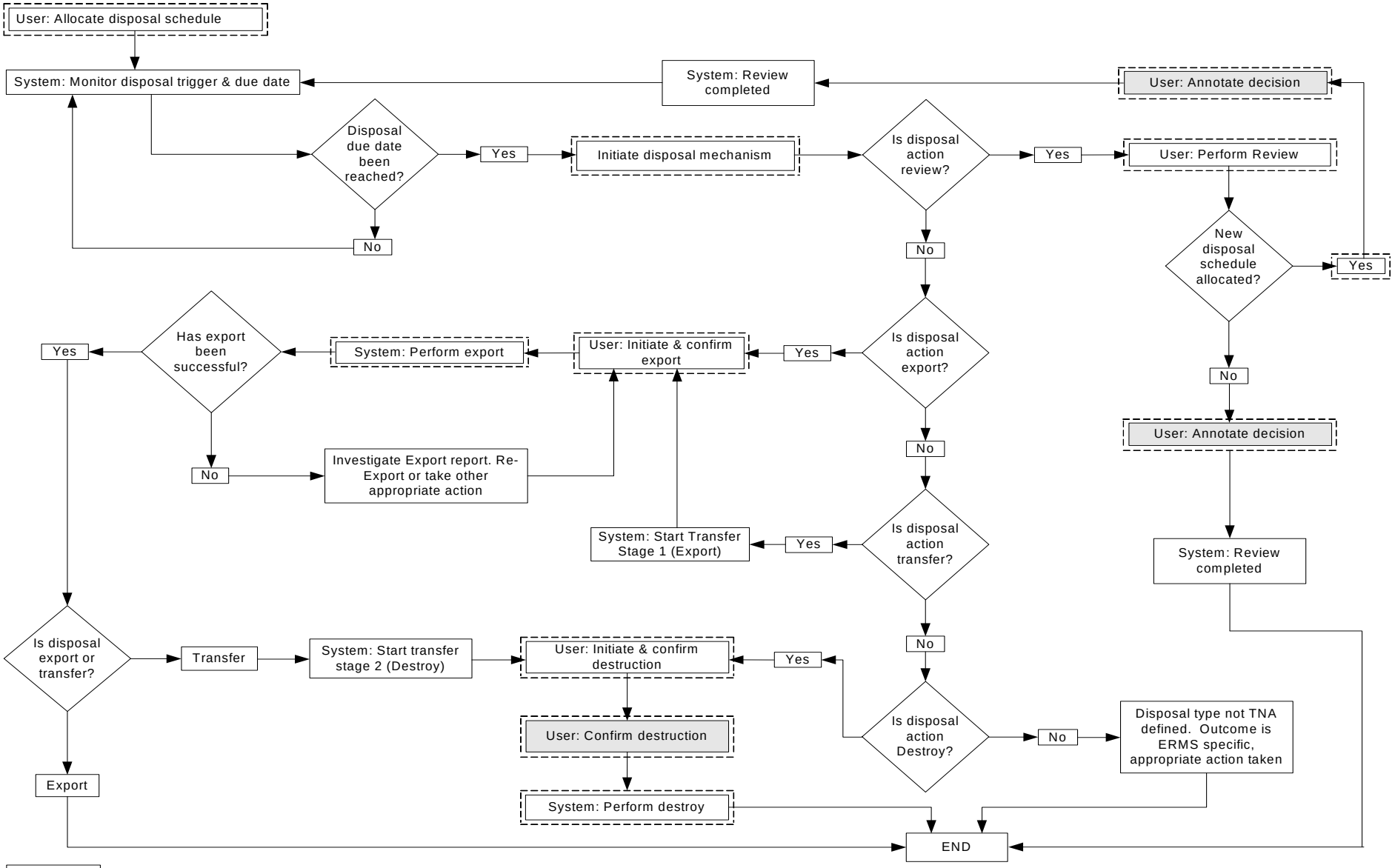


Fig 1.12

This figure illustrates the process for all fileplan objects that have been specifically allocated a disposal schedule. The dashed boxes indicate where audit events are automatically recorded by the ERMS.

Some parts of the figure are shaded to indicate that they are optional.

Where a disposal hold has been applied to a folder or record the ERMS must be able to prevent the execution of a disposal action.

This figure assumes that no disposal conflicts are encountered during the disposal process. Where conflicts are encountered they would need to be properly investigated and resolved by an authorised user prior to the commencement of any disposal schedule execution.

See key for figures on page 23.

EXAMPLE DISPOSAL SCHEDULES

Disposal schedules determine the length of time for which fileplan objects are kept, and the action (e.g. review, export, transfer or destroy) that should be taken on completion of the stated retention period. The time frame may be determined by legislation, business needs, and long-term historical value of records to the organisation and to The National Archives.

Example disposal schedules have been produced by The National Archives for a range of common government records and are accessible from The National Archives website:

http://www.nationalarchives.gov.uk/recordsmanagement/advice/schedules.htm

ACCESS CONTROL MODEL

The access control model inherent in the Requirements for Electronic Records Management systems 2002 is consistent with that required by the Manual of Protective Security[11]. Since these requirements are generic, and intended for applications in a wide range of government organisations, the model does not implement all details of the Manual.

There are two main forms of access control for classes, folders and records:

- hierarchical: limiting access by protective marking security categories.
- non-hierarchical: limiting access by named groups and individuals.

For these, access control is implemented by:

- enabling the allocation of access control markings to classes, folders and records as items of metadata.
- enabling the allocation of access control markings to individual users, named groups of individual users and, optionally, roles to which a user belongs.
- as required, matching all access controls allocated to a class, folder or record with all those allocated to a user (directly, by membership of a group, or by allocation to a role) to determine whether access is allowed or prohibited.

Two further forms of access control are specified in the requirements:

- limiting access to a whole section of classification scheme, and the folders and records classified against it, according to pre-defined named groups of users.
- limiting access to functions (commands and menus) within the ERMS, according to user role.

HIERARCHICAL ACCESS CONTROL

The scheme of protective marking for physical records consists of two main elements:

- A hierarchy of levels describing security categories, from the lowest level to the highest level, where the higher levels encompass all lower levels
- A descriptor, or other qualifying term, which acts as a conditional qualifier to the hierarchical level

[11] The Manual for Protective Marking is a UK government controlled document, and is normally applicable only to UK central Government departments and UK Police Forces. For a more general overview of protective markings see ISO 17799 / BS7799 *Information Security Management.*

SECURITY CATEGORIES

The standard hierarchy of levels is:

- Top Secret (highest level)
- Secret
- Confidential
- Restricted
- Unclassified (lowest level)

Any object can have only one security category marking at any one time; but the setting can change over time.

The majority of records are allocated the lowest level, "Unclassified", and relatively few are allocated the highest level, "Top Secret". A user to whom the highest level is allocated has the greatest breadth of access permissions.

EXAMPLE OF HIERARCHICAL ACCESS CONTROLS

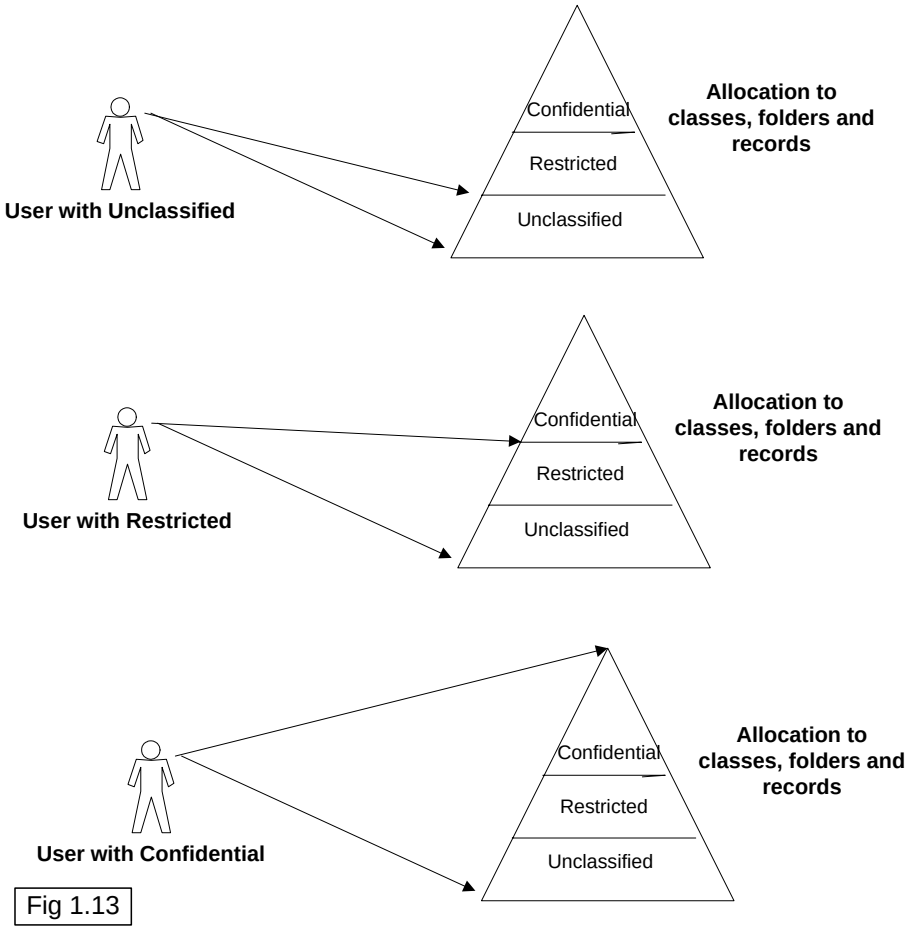


Fig 1.13

For the scenarios illustrated in figure 1.13 on page 61:

- A user allocated a security category of "Unclassified" has access only to classes, folders and records marked as "Unclassified" (unless other controls operate).
- A user allocated a security category of "Restricted" has access (unless other controls operate) to classes, folders and records marked as "Restricted" and "Unclassified".
- A user allocated a security category of "Confidential" has access (unless other controls operate) to classes, folders and records marked as "Confidential", "Restricted" and "Unclassified".

DESCRIPTORS

A descriptor acts as a qualifier on a hierarchical security category, in order to limit access. In principle, a descriptor such as "Commercial in Confidence" implies that the item can only be accessed by users who have the rights to see information so marked. Descriptors are used in conjunction with hierarchical levels other than the lowest: for example, "Restricted: Commercial in Confidence"; "Restricted: Policy; Restricted: Staff".

In the paper records environment, descriptors depend upon interpretation in context to be effective. For example, "Restricted: Staff" requires a potential user to examine the name of the staff member to whom the document is addressed to determine access rights – if that is not the name of the potential user, it should not be accessed. Essentially, it means something like: “If you are not the person named on this envelope, do not open”.

In addition, records with a higher protective marking are normally stored in a separate physical space, so that effective access can be controlled by controlling access to the storage space itself.

This arrangement cannot be made to work in exactly the same way in the electronic environment. Those who are allowed access to items marked with descriptors such as "Staff" cannot feasibly be pre-defined to the ERMS, without creating an unpractical number of variations – including both the staff member receiving the item, and the one from whom it originated. There is unlikely to be a single group of people to whom the descriptor "Commercial in Confidence" applies: membership will vary according to the nature of the material (for example, the particular contract) to which it is applied.

In the electronic world, the descriptor is informative, but cannot in itself be active in controlling access. This is achieved by use of pre-defined access control groups, and ad hoc list of individual user names. For example, the "Staff" descriptor must be implemented, for a particular folder or record, by explicitly naming to the ERMS the originator and recipient to whom access must be limited.

Note: an ERMS can apply a variety of access control markings that provide robust access control along with greater flexibility in the security management of each individual fileplan object. In particular, it should be noted that an ERMS may be able to provide a specific functional security descriptor, which is used along with other access controls to determine access permissions.

NON-HIERARCHICAL ACCESS CONTROL

Limitation of access to specified groups and individuals is achieved by non-hierarchical (flat) access control markings. Both of these markings can be applied together, in as many variations as required.

Pre-defined access groups

A pre-defined access group consist of a list named individuals (users known to the ERMS), that make up a definable and nameable group. Such groups are appropriate to use when the membership remains fairly stable; for example, business unit work teams, Management Board members, and Personnel staff.

The group name can then be applied once, rather than listing each individual separately. It should be noted, however, that there is a management overhead in maintaining up-to-date membership for a large number of access control groups. There is a balance to be struck between the ease of application and the cost of maintenance.

Individual user lists

The ability to apply a list of individual usernames as an access control marking means that ad hoc groupings can be created without adding to this overhead. The list specifies individuals, but has to be created on each occasion.

INTERACTION OF ACCESS CONTROLS

All types of access controls apply together at all times. For example, to access a record marked "Restricted: Personnel" a user must have both the "Restricted" security category and the "Personnel" access control group marking.

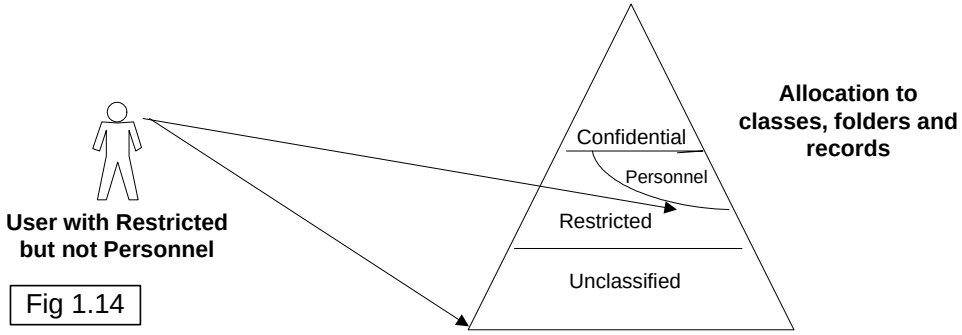


Fig 1.14

In this figure, a user allocated a security category of "Restricted" has access to classes, folders and records marked as "Restricted" and "Unclassified". However, as the user does not have "Personnel" access rights, they do not have access to objects where both controls are applied.

In normal operation, where both a defined access control group and a list of individual usernames are allocated to an item, the list of individual names is treated as an extension rather than a limitation to the members of the named group; that is, the two forms of access control are treated as a Boolean "OR" rather than a Boolean "AND". This is the only exception to the basic rule requiring all necessary access markings to confirm access permission.

For example, access to specified objects may be allowed where the user meets the general requirement:

- (individual user named OR member of an access control group) AND any other access controls are satisfied

USER ROLES

This list of functions is not intended to be definitive and complete, in the sense of listing all possible system functions. It lists only those that are specified in the Requirements for Electronic Records Management systems 2002, either as a relevant mandatory requirement, or to specify limitation to an authorised user.

Symbol Key:

M It is mandatory for a user within this role to be able to carry out this function.

X It is mandatory that a user within this role **cannot** carry out this function.

HD It is highly desirable for a user within this role to be able to carry out this function.

M / X It is mandatory to have the capability to restrict (or not) the ability of a user within this role from carrying out this function as a configuration option.

<space> Users within this role may or may not be able to carry out this function, according to product design.

Function The number in brackets refers to the numbered requirement in volume 1.	**End User**	**Reviewer**	**Local Records Officer**	**Records Manager**	**Systems Administrator**
Add new classes to classification scheme (A.1.4M)	X	X		M	
Mark an empty class as inactive (A.1.7HD)	X	X		HD	
Delete an empty class (A.1.8HD)	X	X	X		HD
Ability to add or amend class metadata (A1.12M)	X	X		M	
Configure pattern of naming classes (A.1.16M)	X	X	X		M
Ability to add or amend folder metadata (A.1.29M)		M	M		
Ability to amend folder metadata in certain fields	M	M	M	M	M
Create new folders (A.1.40M)	M / X	X	M	M	
Close a folder (A.1.42M)			M	M	
Re-open a closed folder (A.1.44M)			M	M	
Re-classify (i.e. move) folders (A.1.47M)				M	
Add reasons for re-classification (A.1.50HD)				HD	

Function The number in brackets refers to the numbered requirement in volume 1.	**End User**	**Reviewer**	**Local Records Officer**	**Records Manager**	**Systems Administrator**
Open new part (A.1.57M)			M	M	
Close a part (A.1.59M)			M	M	
Re-open a closed part (A.1.67M)			M	M	
Capture documents (A.2.1M, A.2.2M, A.2.3M, A2.4M, A2.5HD, A2.6M, A2.7M)	M		M	M	
Declare a document as a record (A.2.13M)	M		M	M	
Amend content of a declared record (A.2.14M)	X	X	X	X	X
Define record_types (A.2.28M)					M
Add / edit metadata to record when declaring (A.2.34M, A.2.40M)	M		M	M	M
Assign vocabulary terms to a record (A.2.36M)	M		M	M	M
Restrict ability to amend record metadata in certain fields (A.2.38M, A.2.41M)	M	M	M	M	M
Re-assign a record to another folder (A.2.50M)			M	M	
Copy an existing record to create a new one (A.2.51M)	M				
Copy an existing record to allocate to an additional folder (i.e. a controlled copy) (A.2.52HD)	HD				
Create and declare an extract (A.2.56HD, A2.57HD)			M	M	
Search for and display records, folders, classes and their metadata (See section A.3 Searching)	M	M	M	M	M
Ability to define and maintain disposal rules (A.4.3M, A4.4M)				M	M
Notify ERMS of external event occurrence (A.4.10M)				M	M
Allocate disposal schedule to a class or folder (A.4.17M)	X	M	M	M	M

Function The number in brackets refers to the numbered requirement in volume 1.	**End User**	**Reviewer**	**Local Records Officer**	**Records Manager**	**Systems Administrator**
Allocate disposal schedule to record_type (A.4.11M)	X			M	M
Allocate schedule to specific record of a specific record_type (A.4.20M)			M	M	M
Re-allocate schedule to folder or class (A.4.21M)	X	M	M	M	M
Place disposal hold (A.4.25M)	X		M	M	M
Initiate and confirm disposal process (A.4.30M)	X		M	M	M
Delete a record outside of disposal function (A.4.65M)	X	X	X	X	M
Delete minimum metadata (A.4.72HD)	X	X	X	X	M
Add and maintain users (A.5.3M)	X	X	X	X	M
Define Access control markings (A.5.6M)	X	X	X	X	M
Maintain user profiles (A.5.16M)	X	X	X	X	M
Define user roles (A.5.17M)	X	X	X	X	M
Define and maintain access control groups (A.5.22M)	X	X	X	X	M
Allocate allowable access controls (A.5.7M, A5.8M, A.5.26M)	M		M	M	M
Modify audit trail data (A.6.5M)	X	X	X	X	X
Configure audit trail tracking (A.6.6HD)	X	X	X	X	M
Run management reports (A.7.1M)			M	M	M
Define pre-set metadata field values (A8.19HD)	X				HD
Configure unique identifier patterns (A.9.4HD)	X				HD
Specify back-up conditions (A.9.13HD)	X		X		HD
Restore system from back-up and forward build (A.9.15M, A.9.16M)	X		X		HD

USER METADATA ELEMENTS

Metadata element	*Obligation Level*	*Repeatable?*
Username	Mandatory	No
Name	Mandatory	No
User rôle	Mandatory	Yes
User business group access permission	Mandatory	Yes
User protective marking security category	Mandatory	No
User descriptor category	Mandatory where applicable	Yes

Notes:

1. The column headed "Obligation Level" indicates whether population of the element is mandatory or optional.
2. The column headed "Repeatable?" indicates whether the element is repeatable (i.e. whether more than one value can correctly be held for it at the same time according to the Metadata Standard)

Retention of Access Control Lists (ACLs)

Departments and agencies will have differing requirements for the retention of access control lists to establish who had access to particular records at what time in the past, depending on the levels of security applicable in their business environment. Neither the Requirements for Electronic Records Management systems 2002, nor the Metadata Standard include this as part of the cross government core requirement.

FLAT LISTING OF METADATA ELEMENTS

This section sets out a 'flat' listing of the metadata elements as identified by specific requirements in the Requirements for Electronic Records Management systems 2002 and the accompanying Metadata Standard. The tables in this section will deal specifically with metadata for:

- electronic classes
- electronic folders
- electronic parts
- electronic records
- electronic record components

A flat listing by entity is a more useful tool for systems configuration than can be adopted in a standard. Although it presents the same content, it does so without the somewhat artificial condensing effect of the **10. Aggregation** element and treats the Metadata Standard's 'sub-elements' as freestanding fields in their own right to clarify, at the systems level, what should actually be happening.

Format of tables [12]

1. The column headed '***M/D Std'***. contains a reference number for each metadata element. This numbering is non-sequential as it corresponds to the numbering of the elements (and sub-elements) in the Metadata Standard. The numbers follow the format **Main element no.sub-element number** except in the case of elements (e.g. ***3.Subject***) that have no sub-elements in the Standard.
2. The column headed 'Ref' gives the numbering for the **Element.Sub-element** as corresponding to the Metadata Standard.
3. The column headed *Metadata element* contains the name for that metadata element corresponding with the naming used in the Metadata Standard.
4. The column headed *Obligation level* indicates whether capture of that element is mandatory or optional.

[12] *The source column for these tables is no longer included in these tables. The information regarding the source of values for metadata elements can be found in the Metadata Standard.*

5. The column headed *Rep?. (Repeatability)* indicates whether the element is repeatable (i.e. whether more than one value can correctly be held for it at the same time according to the Metadata standard)

   "Mandatory where applicable" is best illustrated by way of a few examples:

   - *Example*: An *electronic folder close date* (mandatory where applicable and not repeatable) will not be present until the folder is closed, but must be present exactly once when the folder has been closed
   - *Example*: A *record protective marking security category* may be allocated, or may never be allocated, to an electronic record – but if so, only one security category can be allocated.
   - *Example*: A *review comment* for an electronic folder may not be present at all, or may occur one or more times, depending on the review history of the folder.

   "Mandatory if present" is a term used by the e-GMS. For further detail please refer to the GovTalk website:
   http://www.govtalk.gov.uk/schemasstandards/metadata.asp

6. The source column for these tables is no longer included in these tables. The information regarding the source of values for metadata elements can be found in the Metadata Standard.

CLASS LEVEL METADATA ELEMENTS

Ref	*Metadata element*	*Obligation level*	*Rep? Y / N*
1.1	**Identifier.System ID**	Mandatory	N
1.2	**Identifier.Fileplan ID**	Mandatory	N
2	**Title**	Mandatory	N
3	**Subject**	Optional	Y
4	**Description**	Optional	Y
6.4	**Date.Opened**	Mandatory	N
6.5	**Date.Closed**	Optional	N
9.3	**Relation.Parent object**	Mandatory	N
10.	**Aggregation**	Mandatory	N
13.1	**Rights.Protective marking**[13]	Mandatory	N
13.2	**Rights.Descriptor**[14]	Mandatory if present	Y
14.1	**Disposal.Schedule ID**	Mandatory	N

[13] *Although mandatory this element can be overridden at a lower level in the fileplan (i.e. subordinate class(es) and / or folder(s).*

[14] *Sub-elements 13.9, 13.11, and 13.13 have not been shown here for simplicity. These are mandatory user-defined elements indicating Disclosability but subject to default values of "Yes". See the Metadata Standard for further information.*

Ref	*Metadata element*	*Obligation level*	*Rep? Y / N*
17.1	**Mandate.Authorising statute**	Optional	Y
17.2	**Mandate.Personal data acquisition purpose**	Optional	Y
17.3	**Mandate.DPA exempt category (processing)**	Optional	Y

FOLDER LEVEL METDATA ELEMENTS

Ref	*Metadata element*	*Obligation level*	*Rep? Y /N*
1.1	**Identifier.System ID**	Mandatory	N
1.2	**Identifier.Fileplan ID**	Mandatory	N
2	**Title**	Mandatory	N
3	**Subject**	Optional	Y
4	**Description**	Optional	Y
6.4	**Date.Opened**	Mandatory	N
6.5	**Date.Closed**	Mandatory where applicable	N
6.6	**Date.Cut-off**	Optional	N
9.2	**Relation.Child object**[15]	Mandatory	Y
9.3	**Relation.Parent object**	Mandatory	Y
9.7	**Relation.'See also' relational folder link(s)**	Optional	Y
9.8	**Relation.Hybrid paper folder relational link**	Optional	N
10	**Aggregation**	Mandatory	N
12.1	**Location.Home location**	Optional	N
12.2	**Location.Current location**	Optional	N
13.1	**Rights.Protective marking**	Mandatory	N
13.2	**Rights.Descriptor**	Mandatory if present	Y
13.3	**Rights.Protective marking expiry date**	Optional	N
13.4	**Rights.Custodian**	Optional	N

[15] i.e. =part[s] at this level of aggregation. Minimum mandatory requirement if hybrid folder management offered.

Ref	*Metadata element*	*Obligation level*	*Rep? Y /N*
13.5	**Rights.Individual user access list**	Optional	Y
13.6	**Rights.Group access list**	Optional	Y
13.7	**Rights.Previous protective marking(s)**	Optional	Y
13.8	**Rights.Previous protective marking(s) change date(s)**	Optional	Y
13.9	**Rights.Disclosability to DPA data subject**	Mandatory	N
13.10	**Rights.DPA data subject access exemption**	Optional	Y
13.11	**Rights.EIR disclosability indicator**	Mandatory	N
13.12	**Rights.control.EIR exemption**	Optional	Y
13.13	**Rights.FoI disclosability indicator**	Mandatory	N
13.14	**Rights.FoI Exemption**	Optional	Y
13.15	**Rights.Date of last FOI disclosability review**	Optional	Y
13.16	**Rights.FoI release details**	Optional	Y
13.17	**Rights.FOI release date**	Optional	Y
14.1	**Disposal.Schedule ID**	Mandatory	N
14.2	**Disposal.Disposal action**	Mandatory	N
14.3	**Disposal.Disposal time period**	Mandatory	N
14.4	**Disposal.Disposal event**	Mandatory where applicable	N
14.5	**Disposal.Disposal external event occurrence**	Mandatory where applicable	N
14.6	**Disposal.Disposal (due/effective) date**	Mandatory if present	N
14.7	**Disposal.Disposal authorised by**	Mandatory	N
14.8	**Disposal.Disposal comment**	Optional	Y
14.9	**Disposal.Export destination**	Mandatory if present	N
14.10	**Disposal.Export status**	Optional	N
14.11	**Disposal.Review date**	Optional	N
14.12	**Disposal.Review comment**	Optional	N
14.13	**Disposal.Date of last review**	Optional	N

Ref	*Metadata element*	*Obligation level*	*Rep? Y /N*
14.14	**Disposal.Reviewer details**	Optional	N
14.15	**Disposal.Status (progress) of review**	Optional	N
17.1	**Mandate.Authorising statute**	Optional	Y
17.2	**Mandate.Personal data acquisition purpose**	Optional	Y
17.3	**Mandate.DPA exempt category (processing)**	Optional	Y

PART LEVEL METADATA ELEMENTS

Ref	*Metadata element*	*Obligation level*	*Rep? Y / N*
6.4	**Date.Opened**	Mandatory	N
6.5	**Date.Closed**	Mandatory where applicable	N
6.6	**Date.Cut-off**	Optional	N
9.3	**Relation.Parent object**	Mandatory	N

RECORD LEVEL METADATA ELEMENTS

Ref	*Metadata element*	*Obligation level*	*Rep? Y / N*
1.1	**Identifier.System ID**	Mandatory	N
1.2	**Identifier.Fileplan ID**	Optional	N
2	**Title**	Mandatory	N
3	**Subject**	Optional	Y
4	**Description**	Optional	Y
5	**Creator**	Mandatory	Y
6.1	**Date.Created**	Mandatory	N
6.2	**Date.Acquired**	Optional (Mandatory for email)	N
6.3	**Date.Declared**	Mandatory	N
7	**Addressee**	Optional (Mandatory for email)	N
8.1	**Type.Record type**	Mandatory where applicable	N

Ref	*Metadata element*	*Obligation level*	*Rep? Y / N*
9.1	**Relation.Copy / Pointer**	Mandatory if Present	Y
9.3	**Relation.Parent object**	Mandatory	Y
9.4	**Relation.Redaction/Extract**	Mandatory if Present	Y
9.5	**Relation.Reason for redaction/extract**	Mandatory if Present	Y
9.6	**Relation.Rendition**	Mandatory if present	Y
9.7	**Relation.'See also' relational links**	Optional	Y
10.	**Aggregation**	Mandatory	N
11.	**Language**	Optional	N
13.1	**Rights.Protective marking**	Mandatory	N
13.2	**Rights.Descriptor**	Mandatory if present	Y
13.3	**Rights.Protective marking expiry date**	Optional	N
13.4	**Rights.Custodian**	Optional	N
13.5	**Rights.Individual user access list**	Optional	Y
13.6	**Rights.Group access list**	Optional	Y
13.7	**Rights.Previous protective marking(s)**	Optional	Y
13.8	**Rights.Previous protective marking(s) change date(s)**	Optional	Y
13.9	**Rights.Disclosability to DPA data subject**	Mandatory	N
13.10	**Rights.DPA data subject access exemption**	Optional	Y
13.11	**Rights.EIR disclosability indicator**	Mandatory	N
13.12	**Rights.EIR exemption**	Optional	Y
13.13	**Rights.FoI disclosability indicator**	Mandatory	N
13.14	**Rights.FoI Exemption**	Optional	Y
13.15	**Rights.Date of last FOI disclosability review**	Optional	N
13.16	**Rights.FoI release details**	Optional	Y

Ref	*Metadata element*	*Obligation level*	*Rep? Y / N*
13.17	**Rights.FOI release date**	Optional	Y
14.1	**Disposal.Schedule ID**	Mandatory	N
14.2	**Disposal.Disposal action**	Mandatory	N
14.3	**Disposal.Disposal time period**	Mandatory	N
14.4	**Disposal.Disposal event**	Mandatory where applicable	N[16]
14.5	**Disposal.Disposal external event occurrence**	Mandatory where applicable	N
14.6	**Disposal.Disposal (due/effective) date**	Mandatory if Present	N
14.7	**Disposal.Disposal authorised by**	Mandatory	N
14.8	**Disposal.Disposal comment**	Optional	Y
14.9	**Disposal.Export destination**	Mandatory if Present	N
14.10	**Disposal.Export status**	Optional	N
14.11	**Disposal.Review date**	Optional	N
14.12	**Disposal.Review comment**	Optional	N
14.13	**Disposal.Date of last review**	Optional	N
14.14	**Reviewer details**	Optional	N
14.15	**Status (progress) of review**	Optional	N
15.	**Digital signature (under investigation)**	These Requirements have yet to be finalised	-
17.1	**Mandate.Authorising Statute**	Optional	Y
17.2	**Mandate.Personal data acquisition purpose**	Optional	Y
17.3	**Mandate.DPA exempt category (processing)**	Optional	Y

[16] *A retention period which is* either *time-based* or *event-based,* or *both, will always be present.*

E-MAIL TRANSMISSION DATA MAPPING[17]

Ref.	Mapped to standard metadata element	E-mail Transmission data element	Obligation Level	Rep? Y/N
2	**Title**	Subject line (copy of)	Mandatory	N
5	**Creator**	E-mail sender name	Mandatory	Y
6.1	**Date.Created**	Date / time of transmission	Mandatory	N
7	**Addressee**[18]	E-mail recipient(s)	Mandatory	N
6.2	**Date.Acquired**	Date / time of e-mail receipt	Mandatory	N

COMPONENT LEVEL METADATA ELEMENTS

Ref.	*Metadata element*	*Obligation level*	*Rep? Y /N*
15.1	**Preservation.Originating format**	Optional[19]	N

[17] *Email transmission mapping is not given sequential numbering in its own right in the flat list – see main record level table*
[18] *Element **7Addressee** and sub-element **6.2 Date.Date Acquired** are mandatory for email records **only**.*
[19] *See introductory note on preservation issues in* Metadata Standard

SAMPLE ACCESSIBILITY GUIDELINES

These samples guidelines are indicative only, and are drawn from information available at http://www.maine.gov/oit/accessibility/software_policy.htm:

- A program must provide keyboard access to all functions of the application. All actions required or available by the program must be available without the use of the mouse and with keystrokes, i.e., keyboard equivalents for all mouse actions including but not limited to, buttons, scroll windows, text entry fields, pop-up boxes and pull down lists.
- A program must have a keyboard control sequence among all program controls and focal points (e.g. the sequence of the tab or up/down arrows must follow a logical method of navigating from field to field or up/down arrow to the next list item. In the case of the tab key, the proper format would be from left to right and top to bottom of screen).
- The focus must follow the keystroke, that is, using the arrow keys to navigate through a list followed by pressing the ENTER key or spacebar to select the desired item.
- The software shall not interfere with existing accessibility features built into the operating system, such as Sticky keys, Slow Keys and Repeat Keys.
- Timed responses are not to be used unless an individual user can adjust the timing parameter.
- There shall be selectable visual and auditory indication of key status for all toggle keys (i.e. visual and auditory status indicators for keys such as the Number Lock, Shift/Caps Lock, and Scroll Lock keys).
- The application must allow the user to change the status of toggle keys with keystrokes (e.g. Fully keystroke available menus or facsimile must be provided).
- Keystrokes for all controls should be consistent throughout the entire application. For example, a shortcut key that activates a function on one screen should activate the same function for all occurrences of that function.
- All icons/graphical controls shall have clear precise text labels included on the focus or provide a user-selected option of text-only buttons.
- The use of icons shall be consistent throughout the application. Pull-down menu equivalents must be provided for Icon functions (menu, tool and format bar).
- There must be keyboard access to all pull-down menus.
- Pull-down menu equivalents must be provided for Icon/graphical control functions (e.g. Any icon/graphical control that opens a pull down list and is not directly available with keyboard navigation must have keyboard alternatives to open the same pull down).
- For graphic text, system text drawing tools or other industry standard methods must be used so that screen reader software can interpret the image. Standard text must accompany any graphical representation that includes text.
- A visual cue for all audio alerts must be provided.

- The Sounds feature must be supported where built into the operating system. The user must be allowed to disable or adjust sound volume.
- Information conveyed by audio interface that is not captioned must be available by transcription in a timely manner and must be fully accessible with standard documentation (e. g. Timely should be understood to mean not past the relevance of the audio information conveyed).
- Colour coding is not to be used as the only means of conveying information or indicating an action. An alternative or parallel method that can be used by individuals who do not possess the ability to identify colours must always be provided.
- The application must support user defined colour settings system wide if the development tool allows for this possibility. Highlighting should also be Viewable with inverted colours, Development Tools Permitting.

  Note: Development tools that offer this flexibility are highly recommended.
- No patterned backgrounds behind text or important graphics are to be used.
- User adjustment of, or user disabling of flashing, rotating or moving displays must be permitted to the extent that it does not interfere with the purpose of the application.
- Consistently position the descriptions or labels for data fields immediately next to the field.
- All reports and program output must be available in a format that is accessible by screen readers and other access systems. Examples of accessible text formats are MS Word, MS Excel, straight text and HTML text. PDF documents are not text based and are not recommended.
- All documentation must be accessible through industry standard accessibility tools.
- Accessibility features must be written and provided as part of documentation for the product.

MAPPING OF FUNCTIONAL REQUIREMENTS AND TERMINOLOGY

The National Archives (previously the Public Record Office) Requirements 1999 and 2002, with MoReq and US DoD 5015.2 Standard Requirements 2002 & 2007

This appendix contains information which relates the Requirements for Electronic Records Management systems 1999 and 2002 to corresponding requirements of MoReq and the US DoD 505.2 Standard Requirements 2002 and 2007. It includes tables that relate requirements, followed by one that maps the terminology used in the different publications. Where a requirement number is shown in parentheses, the relationship is approximate and / or partial (e.g. where the TNA functional requirement covers classes and folders but the corresponding requirement covers folders only).

Some of those requirements concerning standards, be they non-functional and / or optional (i.e. requirements numbered A.9.11 and those in sections B.1 onwards) are not mapped. Finally, the US DoD requirements dealing with security (Chapter 4, Management of Classified Records) are not mapped, as they are specific to US military standards.

Where applicable symbols have been used to indicate whether or not a TNA requirement is "Desirable" or "Highly Desirable". Where Applicable this has also been applied to the other standard's requirements.

Note: The symbols used for non-TNA standards is only indicative and may be subject to change by the publisher.

Symbols key

** Highly Desirable (TNA 2002)

^ Desirable (TNA 1999)

* Desirable (TNA 2002)

ə Desirable (MoReq), Non-Mandatory (5015.2)

MAPPING OF TNA REQUIREMENTS TO MOREQ AND DOD

TNA: 2002	TNA: 1999	MoReq: 2001	DOD 5015.2:2002	DOD 5015.2:2007
Record Organisation				
Classification scheme/ fileplan				
A.1.1	A.1.1	(3.1.1)	(C2.2.1.1)	(C2.2.1.1)
A.1.2	A.1.2	3.1.2, (3.1.3)	-	-
A.1.3	A.1.5	3.1.5	(C2.2.1.1)	(C2.2.1.1)
A.1.4	(A.1.2)	3.1.6	-	-
A.1.5	-	3.2.9	-	-
A.1.6	(A.1.12)	3.4.1	-	-
** A.1.7	-	-	-	-
** A.1.8	-	-	C2.2.1.1	(C2.2.1.1)

TNA: 2002	TNA: 1999	MoReq: 2001	DOD 5015.2:2002	DOD 5015.2:2007
A.1.9	-	-	-	-
** A.1.10	^ A.1.22	ə 3.1.8	-	-
* A.1.11	^ A.1.23	ə 3.1.9	(C2.2.3.24)	(C2.2.3.26)
Class metadata				
A.1.12	-	(3.2.1)	C2.2.1.1	C2.2.1.1
A.1.13	-	-	-	-
A.1.14	A.1.3	3.2.2	(C2.2.1.1)	(C2.2.1.1)
A.1.15	(A1.3.)	(3.2.2)	-	-
A.1.16	^ A.1.27	(3.1.4)	-	-
A.1.17	(A.1.4)	-	-	-
A.1.18	(A.1.4)	-	-	-
** A.1.19	-	-	C3.2.2	(C6.2.2)
A.1.20	^ A.1.28	3.2.5	-	-
A.1.21	-	ə 12.1.11	-	-
** A.1.22	-	-	-	-
A.1.23	-	-	-	-
** A.1.24	^ A.1.24	ə 3.2.6	-	-
Folders				
A.1.25	(A.1.2)	3.2.3	-	-
** A.1.26	-	ə 3.2.7	-	-
** A.1.27	^ A.1.26	ə 7.1.6	-	-
A.1.28	-	3.2.9	-	-
Folder metadata				
A.1.29	A.1.15	(3.2.1, 12.1.20)	(C2.2.1.5)	(C2.2.1.5)
A.1.30	-		-	-
A.1.31	-	12.1.2	-	-
A.1.32	-	ə 12.1.11	-	-
** A.1.33	-	-	-	-
A.1.34	-	-	(ə C3.2.1)	(ə C6.2.1)
A.1.35	-	-	-	-

TNA: 2002	TNA: 1999	MoReq: 2001	DOD 5015.2:2002	DOD 5015.2:2007
A.1.36	(A.1.4)	3.2.5	-	-
** A.1.37	^ A.1.24/25	ə 3.2.8	(C2.2.1.2)	(C2.2.1.2)
A.1.38	^ A.2.10	-	C2.2.1.1	C2.2.1.1
Folder management				
A.1.39	A.1.6	3.2.4	-	-
A.1.40	(A.1.6)	-	(C2.2.1.3)	(C2.2.1.3)
A.1.41	A.1.10	3.4.7	C2.2.6.2.1	C2.2.7.2.1
A.1.42	(A.1.10)	-	C2.2.6.2.1	C2.2.7.2.1
A.1.43	-	(3.4.9)	C2.2.8.1.2	(C2.2.9.1.3)
A.1.44	A.1.11	(3.3.6)	C2.2.6.2.2	C2.2.7.2.2
A.1.45	(A.1.12)	-	-	-
A.1.46	A.1.14	3.4.6	C2.2.9	(C2.2.11)
A.1.47	A.1.12	3.4.1, 3.4.3-4	-	-
A.1.48	(A.1.12)	3.4.1	-	-
** A.1.49	-	-	-	-
** A.1.50	-	ə 3.4.5	-	-
* A.1.51	^ A.1.29	ə 3.4.11	(C2.2.3.16)	(C2.2.3.16)
Parts				
A.1.52	(A.1.7)	3.3.1	-	-
A.1.53	-	(3.1.1)	-	-
A.1.54	-	-	-	-
A.1.55	-	12.1.2	-	-
A.1.56	-	3.3.3	-	-
A.1.57	A.1.7	3.3.1	-	-
A.1.58	^ (A.1.29)	-	-	-
A.1.59	A.1.8	3.3.4	-	-
** A.1.60	^ A.1.30	ə 3.4.8	-	-
A.1.61	(A.1.8)	3.3.4	-	-
A.1.62	-	-	-	-
A.1.63	(A.1.9)	3.3.5	-	-

TNA: 2002	TNA: 1999	MoReq: 2001	DOD 5015.2:2002	DOD 5015.2:2007
A.1.64	-	(3.3.2)	-	-
A.1.65	-	-	-	-
A.1.66	-	-	-	-
A.1.67	(A.1.12)	3.3.6	-	-
A.1.68	(A.1.17)	3.4.12	(C2.2.1.4) (C2.2.3.23)	(C2.2.1.7) (C2.2.3.25)
Capture and declaration				
Capture				
A.2.1	(A.2.1)	(6.1.1)	(C2.2.3.1) (C2.2.4.1) (э C3.2.2.3)	(C2.2.3.1) (C2.2.4.1) (э C6.2.2.3)
A.2.2	-	6.3.3	-	-
A.2.3	-	(6.3.1, 10.8.4)	-	-
A.2.4	A.2.5	6.3.2	-	-
** A.2.5	^ (A.2.25)	6.3.4	э C3.2.10	э C6.2.10
A.2.6	A.2.7	-	C2.2.5.3	C2.2.6.3
A.2.7	-	-	-	-
A.2.8	A.2.6	6.1.13	-	-
A.2.9	(A.2.6)	(6.3.2)	(C2.2.4.3)	(C2.2.4.3)
A.2.10	-	э 6.4.2	-	-
A.2.11	-	э 6.4.2	(C2.2.4.3)	(C2.2.4.3)
** A.2.12	-	-	(C2.2.3.19)	(C2.2.3.21)
Declaration				
A.2.13	A.2.2	(6.1.1)	C2.2.3.1	C2.2.3.1
A.2.14	A.2.4	4.5.4	C2.2.3.8	C2.2.3.7
A.2.15	A.2.3	(9.3.1)	C2.2.3.8	C2.2.3.7
A.2.16	-	-	(C2.2.3.2)	(C2.2.3.2)
A.2.17	(A.2.12)	э (6.1.6)	-	(C2.2.4.2)
** A.2.18	-	(10.8.4)	(C2.2.4.2)	(C2.2.4.2)
A.2.19	A.2.16	6.1.8	-	-

TNA: 2002	TNA: 1999	MoReq: 2001	DOD 5015.2:2002	DOD 5015.2:2007
A.2.20	-	6.3.5	-	-
A.2.21	A.1.16	э (6.1.5)	C2.2.3.1	C2.2.3.1
** A.2.22		(3.4.13)	-	-
** A.2.23	-	6.1.15	-	-
A.2.24	(A.1.17)	-	(C2.2.3.23)	(C2.2.3.25)
** A.2.25	^ A.2.31	э 6.1.11	(C2.2.3.15)	(C2.2.3.15)
Record types				
A.2.26	-	-	-	-
A.2.27	-	-	-	-
A.2.28	-	-	-	-
A.2.29	-	-	-	-
Record metadata				
A.2.30	(A.2.8)	6.1.2	C2.2.3.2	C2.2.3.2
A.2.31	-	-	-	-
A.2.32	A.2.8	6.1.3	C2.2.3.21	C2.2.3.23
A.2.33	A.2.11	э 12.1.22	(C2.2.3.10)	(C2.2.3.10)
A.2.34	(A.2.11)	э 12.1.22	C2.2.3.11 (C2.2.3.10)	C2.2.3.11 (C2.2.3.10)
* A.2.35	-	(12.1.9)	-	-
A.2.36	-	э (8.1.10)	(C2.2.3.3)	(C2.2.3.3)
* A.2.37	^ A.2.29	э (8.1.10)	-	-
A.2.38	-		(C2.2.3.22)	(C2.2.3.24)
A.2.39	A.2.12	12.1.23 - .24	-	-
A.2.40	-	-	-	-
A.2.41	(A.2.13)	12.1.20	C2.2.3.22	(C2.2.3.24)
A.2.42	(A.2.13)	9.3.8	-	-
A.2.43	A.2.9	12.1.3/4/21	(C2.2.3.4) (C2.2.3.13)	(C2.2.3.4) (C2.2.3.12)
A.2.44	A.2.14	6.1.7	(C2.2.3.2)	(C2.2.3.2)
A.2.45	A.2.20	(6.1.4), 6.1.9	C2.2.4.2	C2.2.4.2

TNA: 2002	TNA: 1999	MoReq: 2001	DOD 5015.2:2002	DOD 5015.2:2007
A.2.46			-	-
A.2.47	A.2.30	э 6.4.3	C2.2.4.2	C2.2.4.2
A.2.48	A.2.15	(12.1.13)	(C2.2.3.12)	(C2.2.3.11)
A.2.49	A.2.17	(7.1.1-3)	C2.2.3.5	C2.2.3.5
Move, copy extract and relate				
A.2.50	A.1.13	3.4.2	C2.2.3.16	C2.2.3.16
A.2.51	A.2.24	10.3.12	-	-
** A.2.52	(A.1.16)	-	-	-
A.2.53	-	8.1.26	-	-
** A.2.54	-	-	-	-
** A.2.55	^ A.1.31	э 6.1.5	C2.2.3.1	C2.2.3.1
** A.2.56	-	9.3.9	-	-
** A.2.57	-	э 9.3.12	-	-
** A.2.58	^ (A.2.27)	э 9.3.13	-	-
A.2.59	-	-	-	-
** A.2.60	-	9.3.11	-	-
** A.2.61	^ (A.2.27)	э 8.1.26	(C4.2.2)	(C3.2.3)
** A.2.62	-	4.3.6	C2.2.3.18	C2.2.3.18
Bulk import				
A.2.63	-9	6.2.1	э C3.2.2	э C6.2.2
** A.2.64			-	-
A.2.65	-9	-	-	-
A.2.66	-9	6.2.1	-	-
** A.2.67	-9	6.2.2	-	-
Search and Display				
A.3.1	-8	8.1.1	C2.2.1.6	C2.2.1.10
A.3.2	-	-	э C3.2.15	э C6.2.15
A.3.3	A.1.21	3.1.7/8.1.13	-	-
Searching				

TNA: 2002	TNA: 1999	MoReq: 2001	DOD 5015.2:2002	DOD 5015.2:2007
A.3.4	A.1.20	(8.1.4), 8.1.6	C2.2.6.8.2	C2.2.7.8.2
A.3.5	-8	ə 8.1.10	(ə C3.2.9)	(ə C6.2.9)
A.3.6	-	8.1.5	(ə C3.2.9)	(ə C6.2.9)
A.3.7	-8	ə 8.1.9	C2.2.6.8.2	C2.2.7.8.2
A.3.8	-	(8.1.8)	C2.2.6.8.2	C2.2.7.8.2
A.3.9	-8	8.1.8	(C2.2.6.8.2)	C2.2.7.8.2
			(C2.2.6.8.4)	C2.2.7.8.4
A.3.10	-	8.1.7	-	-
A.3.11	-8	ə 8.1.20	-	-
** A.3.12	-	ə (8.1.22)	-	-
A.3.13	-8	8.1.8, 8.1.11	C2.2.6.8.3	C2.2.7.8.3
			C2.2.6.8.4	C2.2.7.8.4
* A.3.14			-	-
A.3.15	-	8.1.17	C2.2.6.8.5	C2.2.7.8.5
A.3.16	A.1.18	8.1.15	-	-
A.3.17	A.1.19	8.1.14	(C2.2.7.8.10)	(C2.2.7.8.10)
A.3.18	B.4.23	8.1.28	(C2.2.6.8.1)	C2.2.7.8.1
** A.3.19	-	-	-	-
Display				
A.3.20	-	8.1.18	-	-
A.3.21	A.2.21	ə 8.2.3	C2.2.6.8.7	C2.2.7.8.6
A.3.22	-	(4.4.3), 8.3.13	(C2.2.6.1.1)	(C2.2.7.1.1)
A.3.23	-	-	(C2.2.7.5)	(C2.2.8.7)
A.3.24	A.2.22	(8.2.1)	(C2.2.3.6)	(C2.2.3.6)
A.3.25	A.2.23	8.3.1	-	-
A.3.26	-	8.3.3	-	-
** A.3.27	-	8.3.4	-	-
A.3.28	-	8.3.2	(C2.2.3.6)	(C2.2.3.6)
Presentation				
** A.3.29	-	-	-	-

TNA: 2002	TNA: 1999	MoReq: 2001	DOD 5015.2:2002	DOD 5015.2:2007
** A.3.30	-	-	(C2.2.1.6)	(C2.2.1.10)
A.3.31	(A.3.38)	-	-	-
** A.3.32	-	-	C2.2.6.8.8	C2.2.7.8.7
Retention and disposal				
Disposal: definition				
A.4.1	^ (A.3.19)	5.1.3, 5.1.1	C2.2.2.1	C2.2.2.1
A.4.2	-	(5.1.3)	-	-
A.4.3	A.3.6	5.1.2	C2.2.2.1	C2.2.2.1
A.4.4	(A.3.15)	(5.1.15)	-	-
A.4.5	-	-	-	-
A.4.6	-	-	-	-
A.4.7	A.3.7 A3.8	5.1.7	(C2.2.2.4) (C2.2.2.4.1) (C2.2.2.4.2) (C2.2.3.2)	(C2.2.2.7) (C2.2.2.7.1) (C2.2.2.7.2) (C2.2.3.2)
A.4.8	A.3.9	5.1.12	-	-
A.4.9	A.3.10	5.1.11	(C2.2.2.7)	(C2.2.2.11)
A.4.10	A.3.11	5.1.11	(C2.2.2.4.3)	(C2.2.2.7.3)
A.4.11	-	-	(C2.2.2.4.4)	(C2.2.2.7.4)
A.4.12	A.3.13	5.1.10	-	-
** A.4.13	-	ə (5.1.5)	C2.2.2.2	C2.2.2.2
Disposal: scheduling				
A.4.14	A.3.1	5.1.4	-	-
A.4.15	A.3.2	5.1.4	-	-
A.4.16	A.3.3	5.1.14	-	-
A.4.17	A.3.6	5.1.16	C2.2.2.6	C2.2.2.10
** A.4.18	-	-	-	-
** A.4.19	-	-	-	-
A.4.20	(A.3.15)	5.1.16	-	-
** A.4.22	-	-	-	-

TNA: 2002	TNA: 1999	MoReq: 2001	DOD 5015.2:2002	DOD 5015.2:2007
** A.4.23	-	-	-	-
A.4.24	^ A.3.20	ɘ 5.1.18	-	-
A.4.25	-	-	C2.2.6.4.1	C2.2.7.4.1
A.4.26	-	-	-	-
A.4.27	-	-	C2.2.6.4.3	C2.2.7.4.3
A.4.28	-	-	-	-
Disposal: execution				
A.4.29	A.3.12	5.1.1	(C2.2.2.5)	(C2.2.2.5)
A.4.30	A.3.14	5.1.8	-	-
A.4.31	(A.3.1)	5.1.6	-	-
A.4.32	(A.3.14)	5.1.13	C2.2.6.6.1	C2.2.7.6.1
* A.4.33	-	-	C2.2.6.6.2	C2.2.7.6.2
A.4.34	(A.3.14)	(5.1.13)	C2.2.2.1	C2.2.2.1
A.4.35	-	-	-	-
A.4.36	-	-	-	-
A.4.37	-	-	-	-
A.4.38	-	-	-	-
Resolving conflicts				
A.4.39	(A.3.36, A.3.35)	5.2.4	-	-
A.4.40	(A.3.34)	5.1.9, 5.2.4	-	-
A.4.41	-	-	-	-
A.4.42	-	-	-	-
A.4.43	-	-	-	-
Review				
A.4.44	A.3.18	5.2.5	-	-
A.4.45	-	5.2.3	-	-
A.4.46	-	5.2.3	-	-
A.4.47	(A.3.18)	(5.2.3)	-	-
A.4.48	^ (A.3.21)	5.2.6	-	-
** A.4.49			-	-

TNA: 2002	TNA: 1999	MoReq: 2001	DOD 5015.2:2002	DOD 5015.2:2007
Export and transfer				
A.4.50	A.3.25	5.3.1	(C2.2.6.5.2) (C2.2.6.5.3)	(C2.2.7.5.2) (C2.2.7.5.3)
A.4.51	(A.3.27)	5.3.2	-	-
A.4.52	A.3.27, A.3.40	5.3.3	-	-
A.4.53	A.3.28	-	-	-
** A.4.54	(B.5.6)	5.3.4	-	-
A.4.55	-	-	-	-
A.4.56	-	-	-	-
A.4.57	(A.3.30)	э (5.3.5)	-	-
A.4.58	-	-	-	-
** A.4.59	-	э 5.3.8	-	-
A.4.60	A.3.31	5.3.6	-	-
A.4.61	^ A.3.44	5.3.17	-	-
A.4.62	^ A.3.43	-	C2.2.6.5.4	C2.2.7.5.4
A.4.63	A.3.32	5.3.7	-	-
Destruction				
A.4.64	(A.3.33)	5.2.7	C2.2.6.6.1 C2.2.6.6.2	C2.2.7.6.1 C2.2.7.6.2
A.4.65	-	9.3.7	(C2.2.5.4)	(C2.2.6.4)
A.4.66	-	-	-	-
A.4.67	A.3.35/45	э 5.3.13	C2.2.6.6.3	C2.2.7.6.3
A.4.68	-	5.3.14	C2.2.6.6.3	C2.2.7.6.3
** A.4.69	^ A.3.46	5.3.15-16	(C2.2.6.6.4)	(C2.2.7.6.4)
** A.4.70	-	(5.3.15)	-	-
** A.4.71	-	-	-	-
** A.4.72	-	-	-	-
A.4.73	-	9.3.7	(C2.2.3.23)	(C2.2.3.25)
A.4.74	-	-	-	-
Access control				

TNA: 2002	TNA: 1999	MoReq: 2001	DOD 5015.2:2002	DOD 5015.2:2007
Access to ERMS				
A.5.1	-	(4.1.2)	C2.2.7.1	C2.2.8.3
** A.5.2	-	-	-	-
A.5.3	-	-	-	-
** A.5.4	-	(4.1.2)	-	-
Access control markings				
A.5.5	B.4.1	-	-	-
A.5.6	B.4.26	(4.1.1)	-	-
A.5.7	(B.4.4)	э (4.1.7)	-	-
A.5.8	(B.4.4)	4.6.1	-	-
A.5.9	B.4.18	4.6.6	-	-
A.5.10	B.4.8	4.1.4	-	-
User profiles				
A.5.11	(B.4.33)	4.1.2, 9.1.8	(C2.2.7.2)	(C2.2.8.4)
A.5.12	B.4.6	4.1.2	-	-
A.5.13	B.4.19	4.6.9	-	-
A.5.14	-	-	-	-
A.5.15	(B.4.8)	4.1.5	-	-
A.5.16	-	4.1.8	-	-
Roles				
A.5.17	B.4.32	4.1.3	C2.2.7 C2.2.7.2	C2.2.8 C2.2.8.2
A.5.18	B.4.33	-	-	-
A.5.19	B.4.34	4.5.1	C2.2.7	C2.2.8
A.5.20	B.4.36	-	-	-
** A.5.21	-	-	-	-
Groups				
A.5.22	(B.4.6)	4.1.4/.6	C2.2.7.3	C2.2.8.5
A.5.23	-	-	-	-
A.5.24	-	(4.1.1), 9.11.7	-	-

TNA: 2002	TNA: 1999	MoReq: 2001	DOD 5015.2:2002	DOD 5015.2:2007
** A.5.25	-	(4.1.2)	(C2.2.7.3)	(C2.2.8.5)
Classes, folders, records				
A.5.26	B.4.4	(4.1.1, 4.6.1)	-	-
A.5.27	(B.4.4)	?	-	-
A.5.28	-	(3.3.3)	-	-
A.5.29	B.4.21	4.6.1/.2	-	-
A.5.30	-	(3.2.5)	-	-
A.5.31	(B.4.22)	э (4.6.5)	-	-
** A.5.32	-	-	-	-
A.5.33	B.4.25	э 4.6.10	-	-
** A.5.34	-	-	-	-
A.5.35	(B.4.22)	-	-	-
A.5.36	(B.4.12)	9.3.3, 9.3.5	-	-
** A.5.37	^ B.4.14	э 9.3.6	-	-
** A.5.38	(B.4.14)	э (4.6.12)	-	-
* A.5.39	-	-	-	-
*A.5.40	-	-	-	-
Custodian				
A.5.41	B.4.7	-	-	-
A.5.42	B.4.11	-	-	-
A.5.43	(B.4.13)	-	-	-
A.5.44	B.4.13	-	-	-
Access control: execution				
A.5.45	B.4.2	-	(C4.1.20)	(C3.1.21)
A.5.46	B.4.20	4.6.8	-	-
A.5.47	(B.4.9)	4.1.1	C2.2.7.3	C2.2.8.5
A.5.48	(B.4.9)	4.1.1	C2.2.7.3	C2.2.8.5
A.5.49	B.4.10	-	C2.2.7.3	C2.2.8.5
A.5.50	(B.4.9)	(4.1.1)	-	-
** A.5.51	^ B.4.15	4.1.9	-	-

TNA: 2002	TNA: 1999	MoReq: 2001	DOD 5015.2:2002	DOD 5015.2:2007
A.5.52	(B.4.23)	4.1.10	-	-
Privacy and opening				
A.5.53	-	-	-	-
Audit				
A.6.1	B.5.1	4.2.1	C2.2.8.1	C2.2.9.1
A.6.2	B.5.1	4.2.4	C2.2.8.1	C2.2.9.1
A.6.3	B.5.8	4.2.6	C2.2.8.1	C2.2.9.1
A.6.4	B.5.2	4.2.2	-	-
A.6.5	B.5.3	(4.2.1)	C2.2.8.6	C2.2.9.6
** A.6.6	^ B.5.10	ə 4.2.7	C2.2.8.2	C2.2.9.2
A.6.7	^ B.5.10	4.2.5, (9.3.14)	-	-
A.6.8	B.5.4	4.2.3	-	-
A.6.9	B.5.5	4.2.8	-	-
A.6.10	B.5.7	-	-	-
A.6.11	-	9.2.2-3	(C2.2.8.3)	(C2.2.9.3)
** A.6.12	B.5.6	4.2.9	C2.2.8.5	C2.2.9.5
Reporting				
A.7.1	-	9.2.1	ə C3.2.4	ə C6.2.4
** A.7.2	-	9.2.7, (5.2.2)	ə C3.2.4	ə C6.2.4
A.7.3	-	9.2.4	C2.2.1.6	C2.2.1.10
A.7.4	-	9.2.4	C2.2.1.6	C2.2.1.10
A.7.5	-	ə (9.2.3)	-	-
A.7.6	-	-	-	-
A.7.7	^ A.1.32	3.4.14	-	-
A.7.8	A.2.33	(9.2.1)	(C2.2.9.5)	(C2.2.11.5)
A.7.9	^ A.3.24, 16-17	5.2.1,8,11	(C2.2.6.1.1)	(C2.2.7.1.1)
A.7.10	-	(9.2.1)	(C2.2.6.5.5)	(C2.2.7.5.5)
A.7.11	-	(9.2.1)	(C2.2.6.6.6)	(C2.2.7.6.6)
Usability				

TNA: 2002	TNA: 1999	MoReq: 2001	DOD 5015.2:2002	DOD 5015.2:2007
A.8.1	(D.10.1)	11.1.4	-	-
A.8.2	-	ə (11.1.4)	-	-
A.8.3	-	-	-	-
A.8.4	-	-	-	-
** A.8.5	(D.10.1)	ə 11.1.2	ə C3.2.5	ə C6.2.5
* A.8.6	^ B.4.35	-	-	-
A.8.7	(D.10.1)	11.1.3	(C2.2.3.12)	(C2.2.3.11)
A.8.8	-	(11.1.3)	(C2.2.3.12)	(C2.2.3.11)
** A.8.9	-	-	-	-
** A.8.10	-	-	-	-
A.8.11	-	11.1.8, 11.1.2	-	-
A.8.12	(D.10.1)	11.1.9	-	-
A.8.13	-	11.1.5	-	-
** A.8.14	-	-	-	-
** A.8.15	-	-	-	-
** A.8.16	-	11.1.7	C2.1.5	C2.1.5
* A.8.17	-	-	-	-
** A.8.18	(D.10.1)	11.1.11, 12.1.16	-	-
** A.8.19	(D.10.1)	11.1.11, 12.1.10	C.2.2.1.2	C.2.2.1.2
A.8.20	-	ə 11.1.13	(ə C3.1.8)	(ə C6.1.8)
A.8.21	-	-	(ə C3.2.3)	(ə C6.2.3)
A.8.22	-	ə 11.1.14	-	-
Design and Performance				
A.9.1	-	11.2.8	-	-
Integrity				
A.9.2	-	(9.1.2)	(C2.2.1.4) C2.2.3.23	(C2.2.1.7) C2.2.3.25
A.9.3	-	7.1.1	C2.2.1.4	C2.2.1.7
** A.9.4	-	ə 7.1.7		

TNA: 2002	TNA: 1999	MoReq: 2001	DOD 5015.2:2002	DOD 5015.2:2007
A.9.5	-	(11.4.7)	C2.1.2	C2.1.2
A.9.6	-	(11.4.7)	C2.1.2	C2.1.2
Interfaces				
A.9.7	-	-	-	-
** A.9.8	-	-	(э C3.2.6)	(э C6.2.6)
* A.9.9	-	-	(э C3.2.6)	(э C6.2.6)
* A.9.10	-	-	э C3.2.7	(э C6.2.7)

TNA: 1999 REQUIREMENTS WHICH ARE NOT MAPPED TO ANY TNA: 2002 REQUIREMENT IN THE MAIN TABLE

A.2.18	(Retain original document title)
A.2.19	(Sequence number)
A.2.32	(Records declared by another)
A.3.4	(Disposal on individual parts)
A.3.22/23	(Workflow module)
A.3.26	(Subsumed in disposal)
A.3.29	(Transfer preparation module)
A.3.37	(Transfer preparation module)
A.3.41/42	(Transfer preparation module)
B.4.24/27-31	(Subsumed – protective markings)
B.5.9	(Superseded – audit trail)
B.5.11	(Superseded – audit trail)

MOREQ REQUIREMENTS WHICH ARE NOT MAPPED TO ANY TNA: 2002 REQUIREMENT IN THE MAIN TABLE

3.2.10	5.3.10	8.1.27	10.3.10	11.4.3
3.4.10	5.3.11	8.1.29	10.3.11	11.4.4
4.1.11	5.3.12	8.3.5	10.4.44	11.6.xx
4.1.12	6.1.12	8.3.7-12	10.5.3	11.7.xx
4.2.10	6.1.14	8.4.1	10.6.5	12.1.1
4.2.12	6.2.3	9.1.1	10.7.2	112.1.5
4.3.7	6.3.6	9.1.5	10.7.3	12.1.6
4.4.1	6.4.1	9.1.6	10.8.1	12.1.12
4.4.2	7.1.4	9.2.8	10.8.2	12.1.14

4.5.2	7.1.5	9.3.1	10.8.3	12.1.15
4.5.3	8.1.2	9.3.2	11.1.6	12.1.17
4.6.3	8.1.12	9.3.4	11.1.10	12.1.18
4.6.4	8.1.19	9.3.10	11.1.15	12.1.19
4.6.11	8.1.21	9.3.14	11.1.6	
5.1.17	8.1.23	10.2.6	11.1.17	
5.2.9	8.1.24	10.3.4	11.1.19	
5.2.10	8.1.25	10.3.8	11.3.xx	

DOD 5015.2:2002 REQUIREMENTS WHICH ARE NOT MAPPED TO ANY TNA: 2002 REQUIREMENT IN THE MAIN TABLE

C2.1.1	C2.2.3.25	C2.2.6.4.2	C2.2.6.8.10	C3.2.11
C2.1.3	C2.2.3.26	C2.2.6.4.4	C2.2.6.8.11	C3.2.12
C2.1.4	C2.2.5.1	C2.2.6.5.1	C2.2.7.4	C3.2.13
C2.1.5	C2.2.5.2	C2.2.6.6.5	C2.2.8.4	C3.2.14
C2.2.1.5	C2.2.6.1.2	C2.2.6.7.1	C2.2.9.4	C3.2.16
C2.2.2.3	C2.2.6.1.3	C2.2.6.7.2	C2.2.9.6	C3.2.17
C2.2.3.9	C2.2.6.1.4	C2.2.6.7.3	C2.2.10.1 - 6	C4.1.xx
C2.2.3.14	C2.2.6.1.5	C2.2.6.7.4	C3.1.1 - 7	C4.2.1
C2.2.3.19	C2.2.6.3.1	C2.2.6.8.6	C3.1.9	
C2.2.3.20	C2.2.6.3.2	C2.2.6.8.9	C3.2.8	

MAPPING OF TNA, MOREQ, AND DOD TERMINOLOGY

The following table relates key terminology in the specifications. Note that in some cases the equivalence is approximate.

TNA: 2002	**TNA: 1999**	**MoReq: 2001**	**DOD 5015.2:2002**
Fileplan	Fileplan	Classification Scheme	File Plan
Entry	Entry	(No direct equivalent)	(No direct equivalent)
(No direct equivalent)	(No direct equivalent)	Level	(No direct equivalent)
Part	Part	Volume	(No direct equivalent)
Instance	Instance	Extract	(No direct equivalent)
Disposal Schedule	Disposal Schedule	Retention Schedule	Disposition Instruction

TNA: 2002	TNA: 1999	MoReq: 2001	DOD 5015.2:2002
Folder	Folder	File	Record Folder
Class		Class	Record Category
Declare	Declare	Classify	Create
Review	Review	Review	Screen

BIBLIOGRAPHY

UK LEGISLATION

- Public Records Act 1958 Chapter 51
  http://www.nationalarchives.gov.uk/policy/act/default.htm
- Data Protection Act 1998 Chapter 29:
  http://www.ico.gov.uk/what_we_cover/data_protection/legislation_in_full.aspx
- Freedom of Information Act 2000 Chapter 36:
  http://www.ico.gov.uk/what_we_cover/freedom_of_information/legislation_in_full.aspx
- Environmental Information Regulations 1992/3240:
  http://www.ico.gov.uk/what_we_cover/environmental_information_regulation/legislation_in_full.aspx

RELEVANT STANDARDS DOCUMENTS

British Standards (BSi)

BSI publications can be are available form their website:

http://www.bsi-global.com/en/Shop/

- British Standards Institution BSi DISC PD0008: 1999 Code of Practice for Legal Admissibility and Evidential Weight of Information Stored Electronically.
- British Standards Institution BSi DISC PD0018: 2001 Code of Practice: Information Management Systems: Building Systems fit for Audit.

International Standards (ISO)

ISO publications are available from their website:

http://www.iso.org/iso/en/prods-services/ISOstore/store.html

- International Standards Organisation ISO 639-2/B Codes for the representation of the names of languages.
- International Standards Organisation ISO 17799 / BS7799 Information Security Management.
- International Standards Organisation ISO 15489 Information and Documentation: Records Management, 2 vols. 2001.
- International Standards Organisation ISO 9001: 2000 Quality management systems: Requirements.
- International Standards Organisation ISO 23950 Information and Documentation: Information retrieval (Z39.50): application service definition and protocol specification.
- International Standards Organisation ISO 2788 Documentation: Guidelines for the establishment and development of monolingual thesauri.
- International Standards Organisation ISO 5964 Documentation: Guidelines for the establishment and development of multilingual thesauri.

- International Standards Organisation ISO 9075 Information technology: database languages: SQL.

OFFICE OF THE e-Envoy PUBLICATIONS

These publications are now accessible via the e-Government unit http://www.cabinetoffice.gov.uk/e-government.

- e-Government data standards catalogue, version 1, UK Office of the e-Envoy, 2002 .
- e-Government interoperability framework [e-GIF] version 4.0, UK Office of the e-Envoy, April 2002.
- e-Government metadata framework [e-GMF], UK Office of the e-Envoy, 2001.
- e-Government metadata standard [e-GMS] version 1.0, UK Office of the e-Envoy, April 2002.
- e-government category lists [GCL], version 1.1, UK Office of the e-Envoy, May 2002.
- e-government: a Strategic Framework for public services in the information age: Guidelines: Security, UK Office of the e-Envoy, 2001.

THE NATIONAL ARCHIVES PUBLICATIONS (http://www.nationalarchives.gov.uk)

(Previously the Public Reference Office)

- Business Classification Scheme Design, TNA 2003. http://www.nationalarchives.gov.uk/electronicrecords/advice/default.htm
- Data Protection Act 1998: A guide for records managers and archivists, PRO 2000. http://www.nationalarchives.gov.uk/policy/dp/default.htm
- Management, appraisal and preservation of electronic records 2 vols, PRO, 1999. http://www.nationalarchives.gov.uk/electronicrecords/advice/default.htm
- Sustainable Electronic Records: Strategies for the maintenance and preservation of electronic records and documents in transition, version 1.0, PRO, 2001. http://www.nationalarchives.gov.uk/electronicrecords/advice/default.htm

OTHER REFERENCES

- CEDARS project / UKOLN, Metadata for digital preservation: the CEDARS project outline specification draft for public consultation, March 2000
- Cornwell Management Consultants plc [for European Commission Interchange of Documentation between Administrations] Model requirements for the management of electronic records 'More' specification, 2001 accessed from http://www.cornwell.co.uk/edrm/moreq.asp.
- DCMI (Dublin Core metadata initiative): http://dublincore.org/.
- National Archives of Australia, Recordkeeping Metadata Standard for Commonwealth Agencies version 1, 1999 accessed from http://www.naa.gov.au/recordkeeping/control/rkms/summary.htm.

- National Archives of Australia, Office of government online, Australian Government Locator Service accessed from http://www.naa.gov.au/recordkeeping/gov_online/agls/summary.html.
- Society of Archivists [UK], Draft Code of Practice under DPA s. 51, 2002 revision, accessed from http://www.archives.org.uk.
- Department of Defense (US) DoD 5015.2-STD Design Criteria Standard for Electronic Records Management Software Applications, June 19, 2002 (undated) and , accessed from http://jitc.fhu.disa.mil/recmgt/standards.html.

- END OF DOCUMENT -