

Requirements for Electronic Records Management Systems

3: Reference Document

Revision : 2002

Requirements for Electronic Records Management Systems

1: Functional Requirements

2: Metadata Standard

3: Reference Document

4: Implementation Guide

Public Record Office
Ruskin Avenue
Kew
Surrey
TW9 4DU
United Kingdom

e-mail: e-records@pro.gov.uk

Website: www.pro.gov.uk/recordsmanagement/

© Crown copyright 2002

3: Reference Document

GLOSSARY OF TERMS	1
ENTITY RELATIONSHIPS	7
DESCRIPTION OF ENTITIES	10
ENTITY LIFE HISTORIES.....	13
EXAMPLE DISPOSAL SCHEDULES	22
USER ROLES.....	23
USER METADATA ELEMENTS	25
ACCESS CONTROL MODEL	26
FLAT LISTING OF METADATA ELEMENTS	29
SAMPLE ACCESSIBILITY GUIDELINES	36
MAPPING OF FUNCTIONAL REQUIREMENTS	37
REFERENCES	48

GLOSSARY OF TERMS

This glossary defines key terms used in the ERMS requirements. The definitions of the entity relationships contained in the earlier section are included.

Some definitions are closely adapted from:

- the terms and definitions in ISO 15489 standard for records management; these terms are marked with an asterisk (*)
- the glossary in BSI DISC PD 0008 code of practice for legal admissibility; these are marked with a double asterisk (**).

aggregation

Generic concept of record assemblies existing at all fileplan levels (in the paper environment the most familiar level of aggregation being the file folder) – see entity relationships in the previous section of this document. Element **16. Aggregation** in the Metadata Standard is where the aggregation level being described by metadata is itself captured as an attribute. The elements and sub-elements applicable to entities at different levels of aggregation differ in a records management metadata scheme.

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.**, so that a sequence of events can be reconstructed in their correct chronological sequence

Note: an audit trail generally consists of one or more lists, or a database which can be viewed in that form.

class (n)

A class is a subdivision of the overall classification scheme by which the electronic 'fileplan' is organised. A class may be sub-divided into one or more lower level classes; and this relationship may be repeated down the hierarchy. A class does not itself contain records; it is an attribute against which a folder is classified.

classification [n] (1)

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*.

classification scheme

A scheme which categorises *records* into assemblies designed to preserve the context of the *records* relative to each other. The full set of classes, at all levels, which together constitute the classification scheme. No assumptions are made about the principles of division, which might be based on functions – activities, subjects, or themes – sub-themes.

classification [n] (2) – see **security category**

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

Note: the term **security category** is used to qualify this meaning of the term in these requirements

component

The smallest aggregation of data managed by an operating system, also referred to (in computer terminology) as a *file* (to avoid confusion, the term *file* has not been used). The full set of physical components from which a logical *Record* is constituted; for example, the multimedia components of a web page (perhaps an HTML stream plus several GIF and JPEG images);. An end user will not interact directly with the component level, but it is necessary to record (automatically) information about components in order to be able to manage them through time, for example, for migration purposes.

Functional Requirements for Electronic Records Management Systems : Reference

Note: the term **Component** has been defined as such for these Requirements; it is not in widespread use elsewhere.

custodian

A person having responsibility for a particular set of records at a particular time, typically a case officer.

cut-off

A fixed period, or recurring date, which defines the point in time at which an electronic part of a folder is closed, and a new part is opened.

Note : for example, an annual cut-off date at the end of each financial year.

declaration

The process of defining that a *document's* contents (and some of its metadata attributes) are frozen as it formally passes into corporate control and is thereby declared as a *record*.

destruction

The process of eliminating records beyond any possible reconstruction*.

disposal schedule

A set of instructions allocated to a *folder* to determine the length of time for which the folder should be retained by the organisation for business purposes, and the eventual fate of the folder on completion of this period of time.

document (n)

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

Note: A document may be on paper, microform, magnetic or other electronic medium. 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 several *components*.

DPA

Data Protection Act 1998. See **References**.

e-GIF / e-Government Interoperability Framework - see **References**

A standard for UK public sector information systems to promote interoperability, published by the Office of e-Envoy. e-GIF incorporates the e-GMF / e-GMS metadata standard.

e-GMS / e-Government Metadata Standard

A qualified Dublin core metadata scheme published by the Office of the e-Envoy within the e-GIF. Based on resource discovery principles.

EIR / Environmental Information Regulations, 1992 – see **References**

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

electronic document

A *document* which is in electronic form.

Note: Use of the term *electronic document* is not limited to text-based documents typically generated by a word processor, but also includes e-mail messages, spreadsheets, graphics and images, html/xml documents, multimedia documents, and other types of office document.

electronic folder

A set of related electronic *records*.

Note: this term is often used loosely to mean *part*.

electronic record

An *electronic document* which has been declared as a corporate record.

element

A metadata attribute applied to an object. A few of the attributes set out in this document operate at the same level as in resource discovery metadata schemes and can be applied directly to records management entities (e.g. 3. Title, 4. Subject). However, in a records management scheme most of the elements are actually applied as attributes to objects at the *sub-element level* (e.g. the sub-elements of 18. Access control, 19. Disposal).

Note: This is necessary to arrive at 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

export

The process of passing copies of a record or group of records with their metadata to from one system to another system, either within the organisation or elsewhere. Export (rather than *transfer*) does not necessarily mean removing them from the first system.

extract / redaction

An *extract* is a copy of a record, from which some material has been removed or permanently masked. An extract is made when the full record cannot be released to a requester, for example under freedom of information, but part of the record can.

An extract of a whole folder is made by creating extracts from some or all of the records which the folder contains.

Note: in the paper environment, an *extract* referred to material removed from a *Record* in the process of making a "*redaction*". This is a concept of little meaning in the electronic environment where there is no need for the physical storage of an extract as a secure redacted version can be made without producing one. In the electronic environment the terms extract and redaction are thus treated as synonymous.

file

This term is not used in isolation, in order to avoid confusion.

fileplan

The full set of classes, and the folders which are allocated to them, together make up a fileplan. The fileplan is a full representation of the business of the organisation, within a structure which is best suited to support the conduct of that business and meet records management needs.

folder

An electronic folder is a (virtual) container for records (which may be segmented by part). Folders are allocated to a class. A folder is the primary unit of management, and is constituted of metadata. Some of this 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.

Where this term is used in isolation, it refers to both electronic folders and paper folders (as the latter are represented in the system). Otherwise, it is used only when qualified, e.g. *electronic folder*, *physical folder* to refer to that specific type of folder.

hybrid folder

A set of related electronic and non-electronic *records*, some stored in an electronic *folder* within the system and some in a non-electronic *folder* (typically, a *physical folder*) outside the system. A hybrid folder may have several *hybrid parts*. Both electronic and non-electronic elements of the hybrid folder must be managed as one.

hybrid part

A set of related electronic and non-electronic *records*, some stored in an electronic *part* within the system and some in a non-electronic *part* (typically, a *physical part*) outside the system. Both electronic and non-electronic elements of the hybrid parts must be managed as one.

inheritance

Principle by which an object can take on a metadata attribute of its 'parent' entity, either by ***Inheritance on creation***

where the subordinate (or 'child') object takes the value of that attribute when it is created; or

or by ***Retrospective inheritance***

where either the attribute of the parent object is changed or the parent object is altered (e.g. by moving a folder in the fileplan so that it has a new parent object).

marker

Metadata which describes attributes of a *record* which is stored externally to the system (for example, large paper documents such as building plans, a database held outside the ERMS, a record on a CD-Rom).

metadata

Information describing the context, content and structure of records, folders and classes

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*.

MoREQ / Model requirements for Recordkeeping – see References

Requirements for EDRM produced by an EC-funded project; not specific as to sector or format. See *References*

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 – which, until and unless a second part is created, is co-extensive with the whole folder. The concept of parts allows the contents of folders which would otherwise be closed to be disposed of in a regular and orderly manner.

Note: Strictly speaking, records are contained within a part, although a particular system may present an interface which depicts records as contained directly within a folder.

permanent preservation

The process by which *records* are preserved in perpetuity in the national archive, in an accessible and reliable form and maintaining them as authentic records, reflecting their business context and use.

physical folder

A physical folder is an entry within the fileplan for a legacy physical, usually paper, folder. The folder is not itself held within the system, but is located elsewhere.

There are two types of case in which a physical folder is represented:

- where the physical folder stands on it own, and has no relationship with an electronic folder, other than being allocated the same classification
- where the physical folder is the physical equivalent of an electronic folder, and has the same title; the physical and electronic folder together constitute a hybrid folder.

pointer

Method of controlling instances of electronic records classified against more than one folder, without physical duplication of the document. More than one pointer can be created within the fileplan to reference a single database object, but each must be logically managed as though separate records for disposal.

presentation

Process of publishing records, folders and their metadata from the ERMS for 'presentation' outside the ERMS environment (e.g. for publication on a website) by methods within ERMS control.

protective marking

Designations applied to a *record* to show the degree of security that it should be afforded. One of several words and/or phrases taken from controlled lists, which indicate the access controls applicable to a record.

Note: see the separate descriptions of protective markings in the Security model for further definition.

record (n)

'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'*.

In these requirements, a record is a *document* which has been declared as a formal record, constituted of both content and metadata.

record type

A definition of a record object which specifies particular metadata attributes and particular forms of behaviour. A default record type is the norm, specific record types are deviations from the norm. Specifically, this concept is used for the purposes of complying with the fair processing provisions of the Data Protection Act 1998 to enable different disposal behaviour of records created as instances of a limited number of pre-defined record types.

redaction / extract

See *extract / redaction*

refinement

Term used in qualified *DC* metadata schemes (including *e-GMS*) to 'refine' the meaning of the main *element* for a particular usage. 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 (see *Element*) many of which will apply to the same entity, whilst not implying a narrower scope than the main element.

Note: For example, in the *e-GMS*, "Description.Abstract" is a refinement of the *element* "Description"

rendition

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.

resource discovery

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

review (n)

The examination of the disposal status of a *folder*, or a *part* of a folder, to determine whether its disposal can now be determined where this has not previously been possible (i.e. that it should be destroyed, sent to an archive, or retained for a further review at a later date in circumstances).

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

rôle

The aggregation of functional permissions granted to a predefined subset of system users.

Note: an example of a rôle is *records manager*. The records manager rôle has permissions to access many, but not all, administration functions and most record creation and access functions; the rôle is associated with all users who have records manager tasks.

sub-element

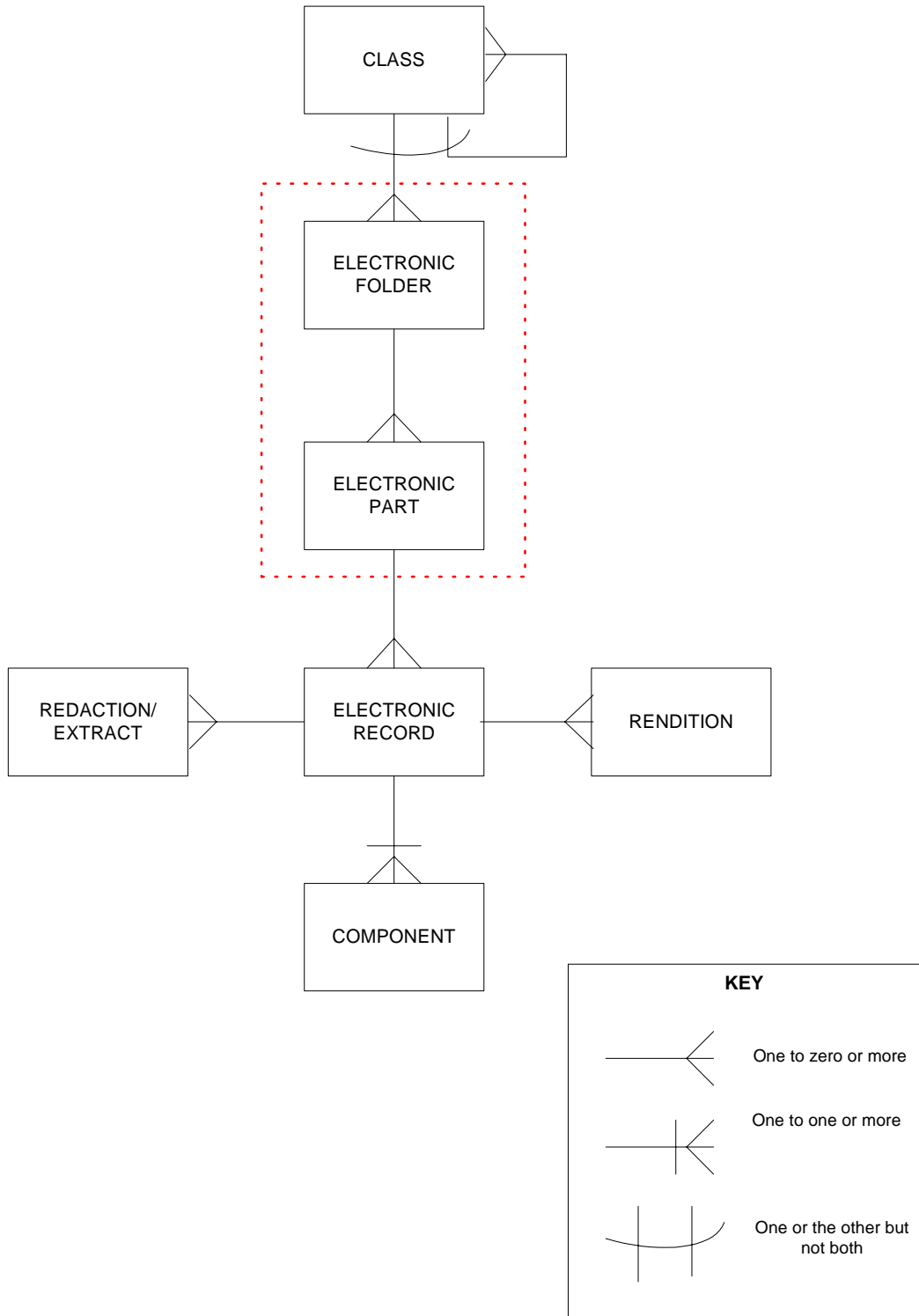
Metadata attribute applied to certain records management entities, roughly equivalent to *Refinement* in the *e-GMS*. See *Element* for further explanation.

transfer

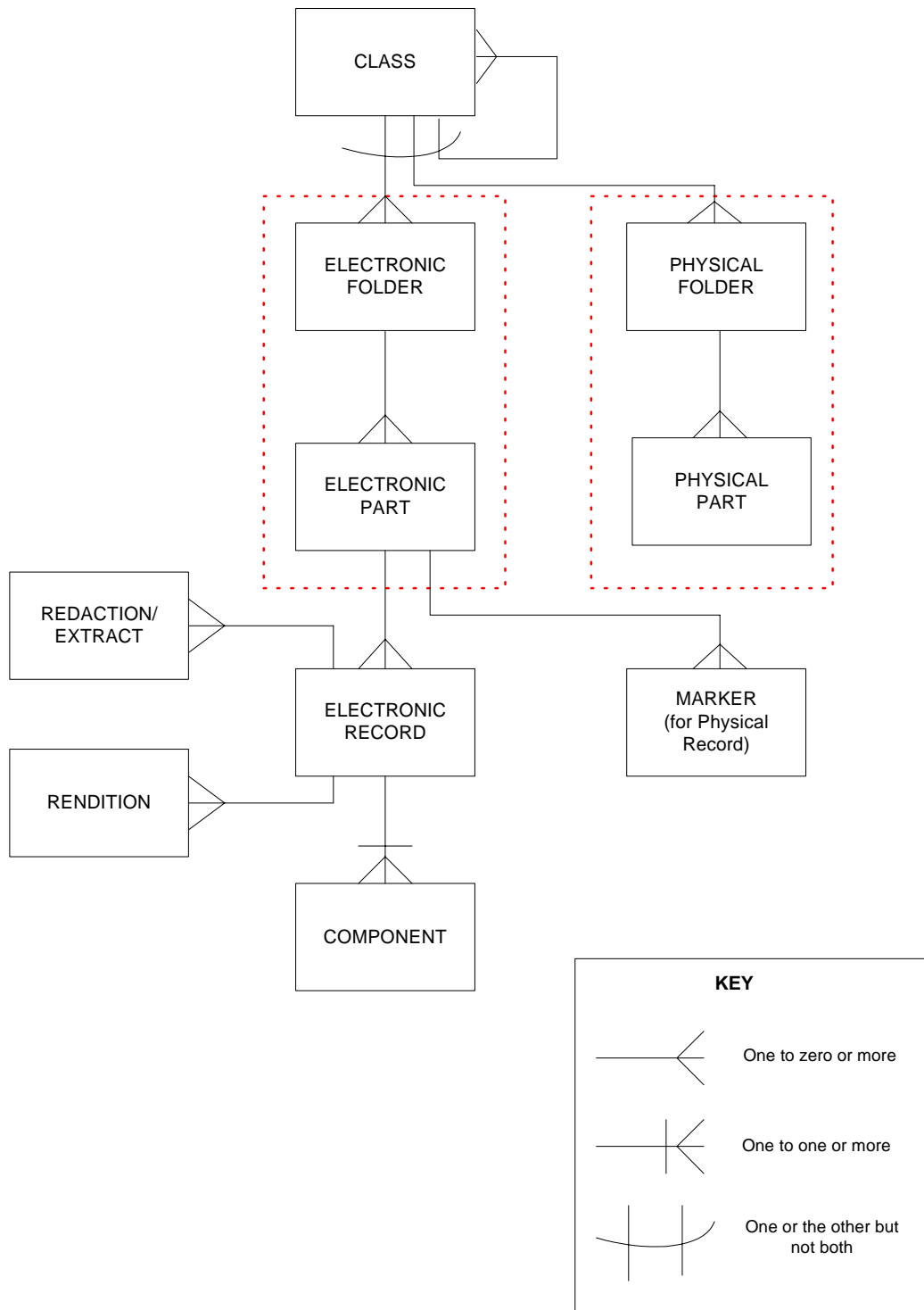
The process of *exporting* (usually groups of) complete electronic folders and subsequently destroying them within the exporting system, effectively transferring custody of the records. Records may be transferred for the purpose of permanent preservation in the Public Record Office, or some other place of deposit; or following structural changes to the machinery of government which create, dissolve or merge organisations.

ENTITY RELATIONSHIPS

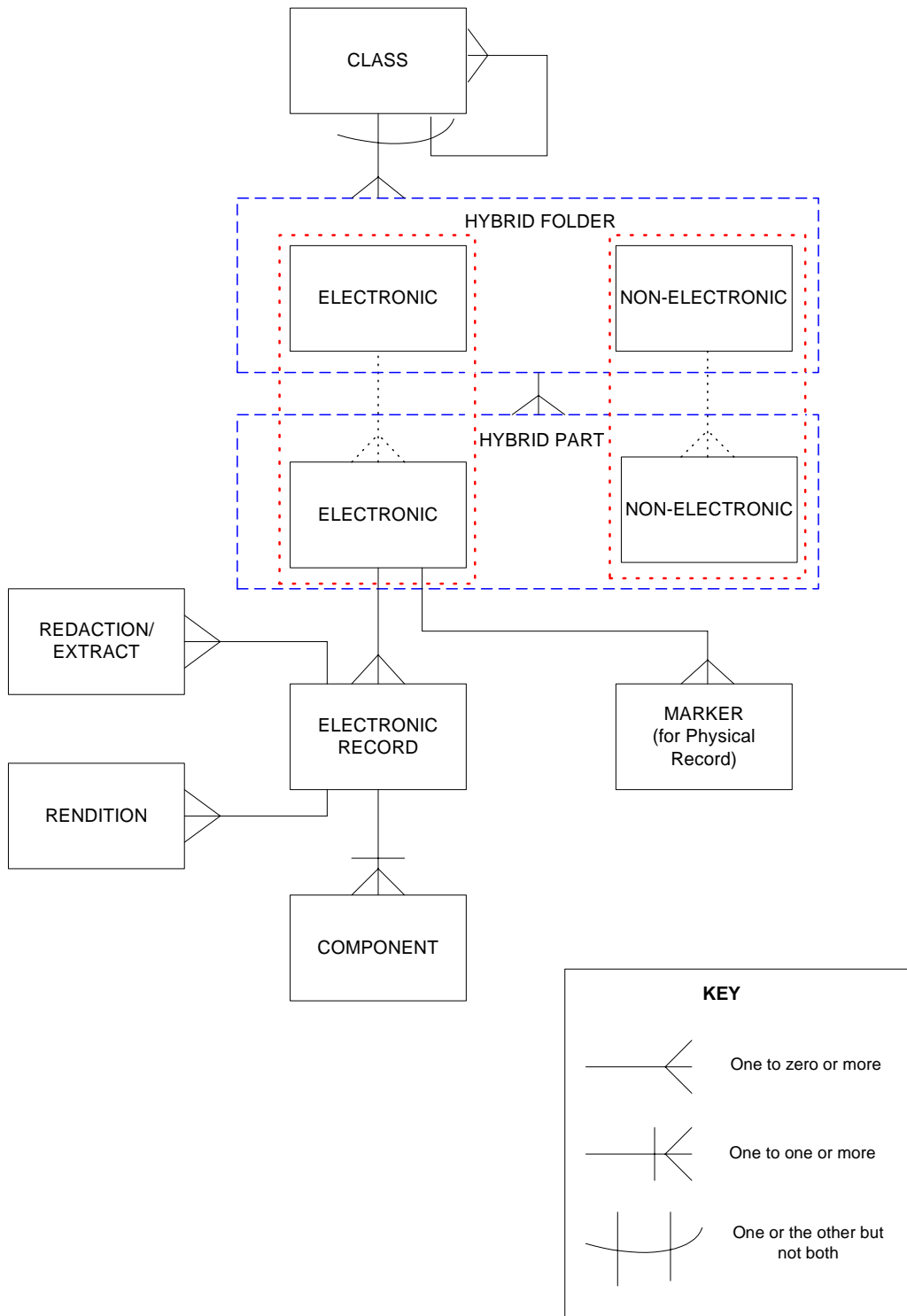
ENTITY - RELATIONSHIPS 1 : ELECTRONIC



ENTITY - RELATIONSHIPS 2 : ELECTRONIC and PHYSICAL



ENTITY - RELATIONSHIPS 3 : HYBRID



DESCRIPTION OF ENTITIES

CLASS

A class is a subdivision of the overall classification scheme by which the electronic 'fileplan' is organised. No assumptions are made about the principles of division, which might be based on functions–activities, subjects, or themes–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 lower level classes; and this relationship may be repeated down the hierarchy. This is the arrangement by which the majority of government departments continue to organise their records. A hierarchical classification must be possible, but is not mandated in implementation.

The full set of classes, and the folders which are allocated to them, together make up a fileplan. The fileplan is a representation of the business of the organisation, within a structure which is best suited to support the conduct of that business and meet records management needs. A class does not itself contain records; it is constituted of metadata, some of which may be inherited down the hierarchy.

FOLDER

A folder is a (virtual) container for records (which may be segmented by part). Folders are located in the fileplan by being allocated to a class (i.e. by being classified). A folder is the primary unit of records management, and is constituted of metadata. Some of this metadata may be inherited from the class to which the folder belongs; and some folder metadata may be inherited by the records which the folder itself contains.

There may be many folders within a single class (or none, if no folders have yet been created at that point). The primary focus of these documents is on management of the electronic folder, although physical folders are allowed for.

PHYSICAL FOLDER

A physical folder is an entry within the fileplan for a physical or paper folder, which is not itself held within the system, but is located elsewhere. Such an entry provides information about the folder and its location. A physical folder will be classified in the same way as an electronic folder, and under the same classification scheme.

There are two types of case in which a physical folder is represented:

- where the physical folder stands on it own, and has no relationship with an electronic folder, other than being allocated to the same class
- where the physical folder is the physical equivalent of an electronic folder, and has the same title; the physical and electronic folder together constitute a hybrid folder. This case is indicated in the diagram by a dotted line; hybrid folders must be managed as one for purposes of retrieval and disposal.

PART

A part is a segment of a folder. The folder is segmented for management purposes only, and is managed from the folder level. A folder will contain at least one – the initial – part, which, until and unless a second part is created, is co-extensive with the whole folder. For organisations which choose not to make use of the part functionality, all folders will be of this nature; effectively, for practical purposes of the end user, the part may not be an entity which the end user interacts directly – see red dotted line in diagrams 2 and 3.

A folder may contain many parts. In cases where part functionality is used, the end user will work with the most recent part; however, the distinction between parts will remain important for the correct management of disposal.

Strictly speaking, records are contained within a part, although in some cases an interface may present records as contained directly within a folder.

RECORD

A record is the logical entity which has been declared as a formal record. The record is constituted of both content and metadata; it may be a single object, such as a Word document, or a set of closely bound objects which are meaningfully treated as one, such as a web page or multimedia document. A folder and part(s) may (and is expected to) contain many records; a newly created folder may not yet contain any records.

A record may inherit some of its behaviour from the folder to which it is assigned, in particular in relation to disposal. A document may be allocated to more than one folder, thus creating more than one record; each allocation is treated as a separate record for management purposes: for example, it may display different disposal behaviour in the context of different folders. It is important to retain this distinction in concept, even though it is a single electronic file that has multiple allocations.

MARKER (for a physical record)

A marker is an entry for a physical record, which is made in an electronic folder. The record itself is held outside of the system; a marker is the metadata for that record. A marker is not expected to be used for a simple paper record, which would normally be held in a physical folder, without additional description. Typically, a marker might be used to describe items such as large building plans, videotapes, or a database, which can neither be contained in a conventional physical file or easily digitised.

In this model, a physical folder cannot contain markers for physical records.

EXTRACT (REDACTION)

An extract is a copy of a record, from which some material has been removed or permanently masked. An extract is made when the full record cannot be released to a requester, for example under freedom of information, but part of the record can. Most records will never have an extract made from them; some records may have several different extracts made at different times, as the sensitivity of the material decreases.

An extract of a whole folder is made by creating extracts from some or all of the records which the folder contains.

COMPONENT

A component is the set of physical components from which a logical record is constituted; for example, the multimedia components of a web page. An end user will not interact directly with the component level, but it is necessary to record (automatically) information about components in order to be able to manage them through time, for example, for migration purposes.

The Component entity is shown here for completeness, but these functional requirements and accompanying metadata model do not address component management beyond initial recognition. Requirements for sustainability, to be published in 2002/2003, will set out the component level in more detail.

HYBRID FOLDER

A hybrid folder is a folder which has both electronic and non-electronic elements, both of which have entries in the ERMS. The non-electronic folder is typically a physical, or paper,

folder; but unlike a physical folder which is a separate entity and can have an independent allocation to a class, both the electronic and non-electronic elements of a hybrid folder must have the same single allocation to a class. A hybrid folder is managed as a single logical entity, but will have slightly different metadata for each element (e.g. the non-electronic element will have location information). The dashed blue line in diagram 3 indicates this relationship.

HYBRID PART

A hybrid part is a part of a hybrid folder, which has both electronic and non-electronic elements. Both electronic and non-electronic elements of the part must be managed as one – shown by the dashed blue line in diagram 3 – in particular ensuring that both elements are co-ordinated and co-extensive. for example, the electronic element of *part 2* of a hybrid folder is always associated with the non-electronic element of *part 2*, and both have the same open and close dates.

ENTITY LIFE HISTORIES

Electronic folder entity life history

This section presents the entity life history of an electronic folder. The entity life history diagrams show the evolution of a folder from initial creation, through the addition of records to one or more parts, and management and maintenance of the folder, to its eventual destruction or permanent preservation in an archive as a complete folder with all the records which it contains.

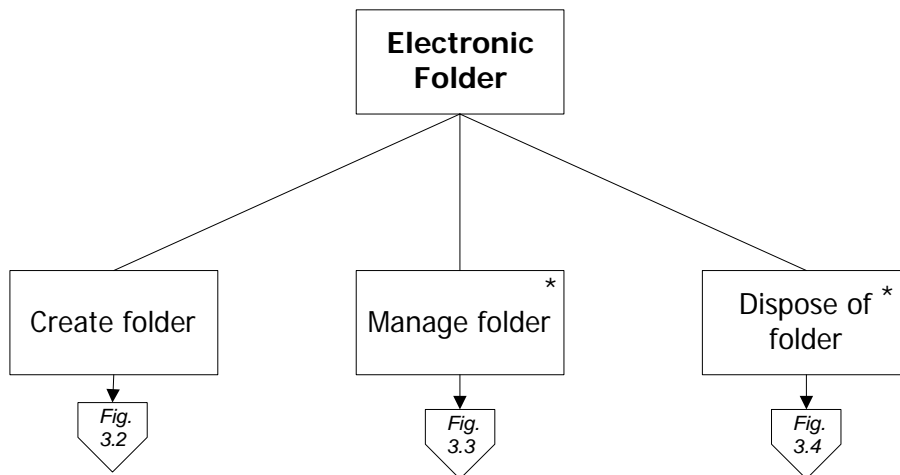


Fig. 3.1: Electronic folder entity life history

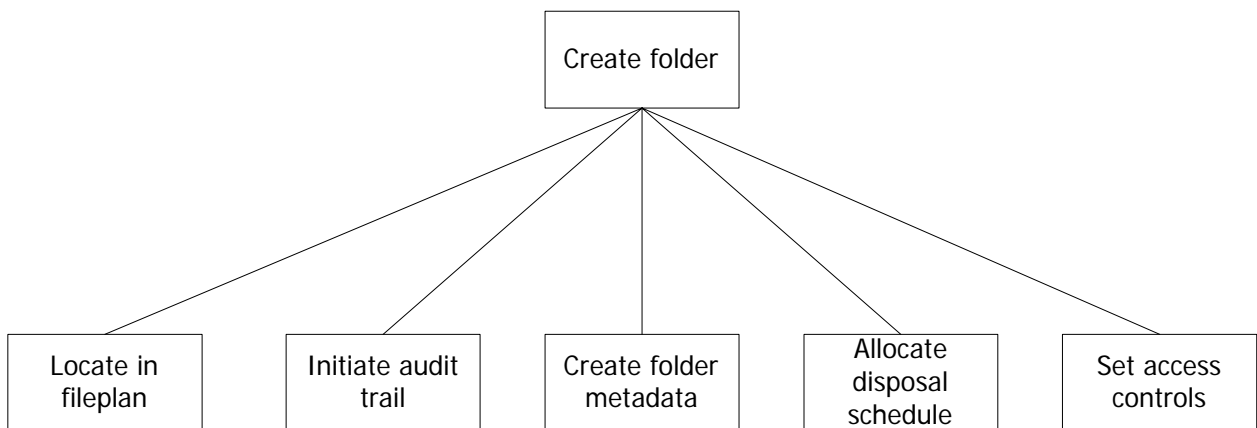


Fig. 3.2 : Create electronic folder

In the diagram boxes, a * character indicates an *iteration* of zero to many times, and a ⁰ character indicates a *selection* amongst the options available in that group.

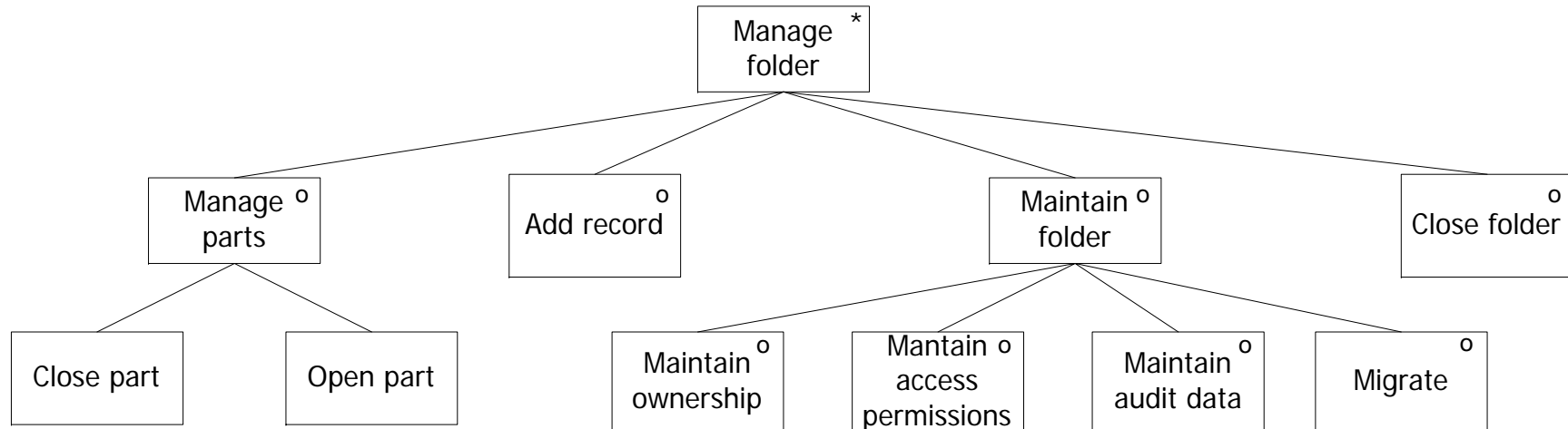


Fig. 3.3: Manage electronic folder

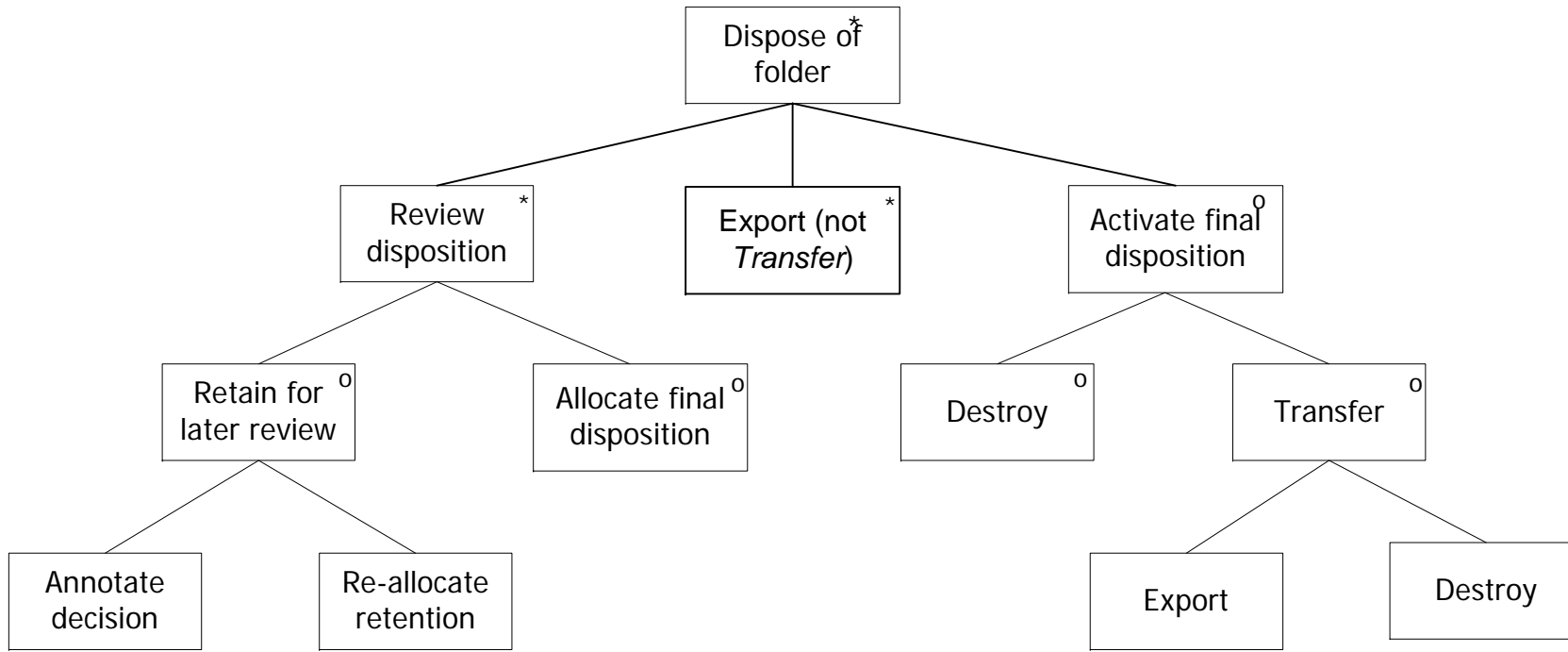


Fig. 3.4: **Dispose of electronic folder**

Commentary : Folders

Key concepts

- a record is, by default¹, governed by the folder with which it is associated for purposes of management and disposal
- by default¹, complete folders of records are managed and disposed of as a whole, without selective removal of records
- folders of records must be maintained over time, even if closed for addition of records
- access controls may be applied separately both to folders and to records within that folder.

Life history events

Each event in the above diagrams are briefly described below. The events are in alphabetical order.

Activate final disposition

A final disposition is one of either destroy or transfer. Following completion of a final disposition, the folder is removed from the system.

Add record

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

Allocate disposal schedule

A disposal schedule is allocated to the folder, which will apply to all records it will contain. A disposal schedule will include a retention period and instructions for disposition at conclusion of that period: one of either *review*, *destroy* or *transfer*.

Allocate final disposition

Disposition instructions of either destroy or transfer are allocated to the folder following a review.

Annotate decision

Desirably, the reasons for a review decision to retain a folder are included with the folder metadata for use in later reviews.

Audit trail data

The folder audit trail is updated as it is accessed, maintained, etc.

Close part

The currently open part is closed so that no further records can be added to it, and if the folder as a whole is not also closed, a new part is opened.

Close folder

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

Create folder

The folder is created, and is made ready to receive records.

Create folder metadata

The specific folder metadata is created for this folder, as configured for this implementation. Note that folder titles / reference codes, disposal schedules and access markings are also metadata elements but are separated here for clarity.

¹ The only permissible exception to this is where a specific record type has been defined and implemented in the ERMS. See Functional requirements

Destroy

The folder is destroyed; during this destruction, some of the metadata should be retained.

Dispose of folder

The folder will be disposed of by one of the actions lower in the diagram, according to the disposal schedule which has been set at the point of creation, or by a previous review. Note that the review process may occur as many times as necessary, but a final disposition (destroy or transfer) will only occur once.

Export

A copy of the folder containing copies of the group of records it contains is passed (with the metadata) to from one system to another system, either within the organisation or elsewhere. Export (rather than *transfer*) does not necessarily mean removing them from the first system.

Initiate audit trail

The audit trail to records events which occur to this folder is initiated.

Locate in fileplan

The folder is located at a point within the fileplan structure, and allocated a reference code and title, as required.

Maintain access permissions

Access permissions to the folder as a whole may be changed during the its life (whether open or closed), as its contents become less sensitive.

Maintain audit data

Audit data will be maintained for both open and closed folders.

Maintain folder

The folder must be maintained through its life, whether open or closed.

Maintain ownership

Ownership of the folder may change as individuals and business units change.

Manage folder

The folder is managed through its life, by the addition of parts and records during its active life, and continued maintenance when the folder has been closed.

Manage parts

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

Migrate

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

Open part

A new part is opened within the folder, following closure of the most recent part, unless the folder itself is closed.

Re-allocate retention

As a consequence of the review decision, a retention period is re-allocated to the folder, which will cause it to be reviewed again at a later date.

Retain for later review

The reviewer decides to retain the folder and schedules a later review by the actions below.

Review disposition

The folder is reviewed to assess its disposition; the outcome can be to retain for further review, to destroy or to transfer to the Public Record Office. A folder may be subject to more than one review.

Set access controls

The initial access controls (including protective markings) for the folder as a whole are set.

Transfer

The folder (more usually groups of folders) and all its contents and metadata, is transferred by *exporting* and subsequently destroying it within the exporting system, effectively transferring custody of the records. Records may be transferred for the purpose of permanent preservation in the Public Record Office, or some other place of deposit; or following structural changes to the machinery of government which create, dissolve or merge organisations.

Electronic record entity life history

This section presents the entity life history diagram of an electronic record. The Entity life history diagram shows the evolution of a document, from origination, through its transformation into a record, to its eventual destruction or permanent retention in an archive as part of a complete folder.

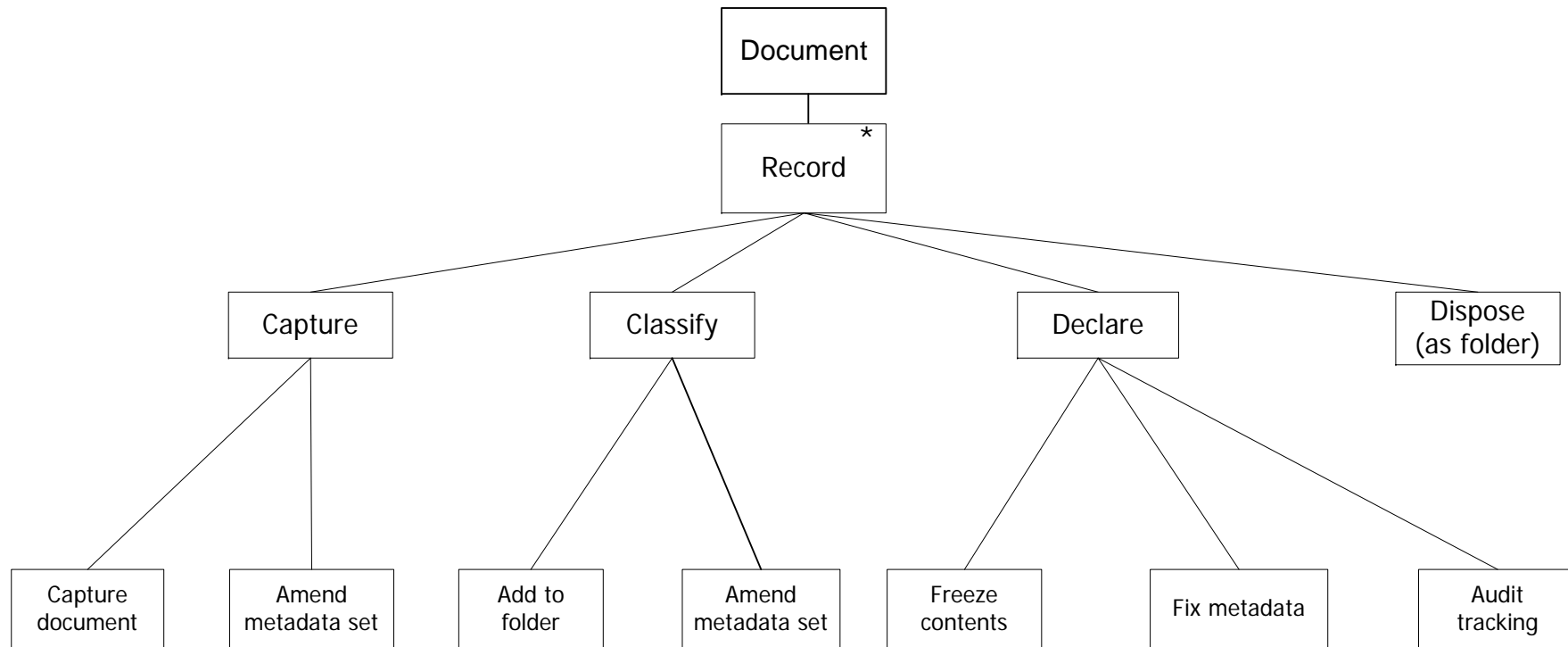


Fig. 5.1: Record life history

Commentary : Records

Key concepts

- a version of a document may be declared to be a record at any time
- record *contents* cannot be changed (but some of their metadata, e.g. protective marking, can be changed)
- once classified to a folder in the fileplan, a record will be disposed of according to the schedule for that folder .

Life history events

Each event in the above diagram is briefly described below. The events are in alphabetical order.

Access control marking

The protective marking, or other access control marking, of the record is changed; usually to downgrade it because its sensitivity has decreased with time.

Add to folder

The action of adding a record to a folder within the fileplan classifies it against the classification scheme that the fileplan represents.

Amend metadata set

The metadata associated with the content in the document management environment may be inappropriate or unhelpful for the document in the process of becoming a record. Whilst it is desirable for such properties as creator to be offered as the default at this point, the acceptability of the values need to be reviewed at this point and amended prior to declaration. Similarly some of the metadata arising from the action of classifying the record (mostly inherited from the fileplan) may require amendment where permissions exist (e.g. access control).

Apply changes

The document is changed (i.e. edited); and/or annotations are applied (analogous to hand written marginal annotations on paper documents); and/or the document is linked to other folders. This represents normal development and/or maintenance of a document which is not (yet) a record.

Audit tracking

The record's audit trail is updated as it is accessed, copied etc.

Capture

A record is originated as a document and brought within the records management environment.

Change metadata

The record's metadata is updated, in the ways defined below; note this is optional.

Classify

The process by which a document or record is added to one or more folders; this may occur at the same time as *declaration*, or may precede the declaration process where an ERMS allows this.

Create

The document is produced in electronic form, often using a text processor or e-mail program.

Declare

The owner of the document defines that the document is now a corporate record. This process triggers the events below it in the diagram structure.

Determine metadata inherited by default

A large proportion of record level metadata will, by default, be inherited from its position in the fileplan (see *classify*). Some of this – e.g. access control metadata – will be editable where for some reason this inherited value needs to be overridden.

Disposal as folder

The record is subject to review and disposition (which will finally result in either destruction or transfer to the Public Record Office) as part of actions applied to the complete folder in which it is stored. During the destruction process, some of the folder level metadata should be retained.

Record

This is not an entity or event. It is the context of the diagram, and indicates that the diagram illustrates the life history of records.

Fix metadata

Most of the metadata (especially the system generated metadata) is made read-only. This is essential to transform a document into a record

Freeze contents

The contents of the document are made read-only. This is a mandatory first step to transform a document into a record.

EXAMPLE DISPOSAL SCHEDULES

Disposal schedules determine the length of time for which records are kept, and the action which should be taken on the records at completion of that period. Disposal schedules may be determined by legislation which stipulates retention periods, by business needs, and by long-term historical value of the records to the organisation and to the national archives.

Example disposal schedules have been produced by the Public Record Office for a range of common government records and are accessible from the PRO website:

<http://www.pro.gov.uk/recordsmanagement/standards>

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 which are specified in the Functional Requirements, 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	End User	Reviewer	Local Records Officer	Records Manager	Systems Administrator
The number in brackets refers to the numbered requirement in volume 2					
Add new classes to classification scheme (A.1.4)	X	X		M	
Mark an empty class as inactive (A.1.7)	X	X		HD	
Delete an empty class (A.1.8)	X	X	X		HD
Ability to add or amend class metadata ((A1.1.2)	X	X		M	
Configure pattern of naming classes (A.1.16)	X	X	X		M
Ability to add or amend folder metadata (A.1.29)		M	M		
Control ability to amend folder metadata in certain fields	M	M	M	M	M
Create new folders (A.1.40)	M/X	X	M	M	
Close a folder (A.1.42)			M	M	
Re-open a closed folder (A.1.44)			M	M	
Re-classify (i.e. move) folders (A.1.47)				M	
Add reasons for re-classification (A.1.50)				HD	
Open new part (A.1.57)			M	M	
Close a part (A.1.59)			M	M	
Re-open a closed part (A.1.67)			M	M	
Capture documents (A.2.1 – 7)	M		M	M	
Declare a document as a record (A.2.13)	M		M	M	
Amend content of a declared record (A.2.14)	X	X	X	X	X
Define record_types (A.2.28)					M
Add / edit metadata to record when declaring (A.2.34) (A.2.40)	M		M	M	M

Functional Requirements for Electronic Records Management Systems : Reference

Function	End User	Reviewer	Local Records Officer	Records Manager	Systems Administrator
The number in brackets refers to the numbered requirement in volume 2					
Assign vocabulary terms to a record	M		M	M	M
Restrict ability to amend record metadata in certain fields (A.2.38) (A.2.41)	M	M	M	M	M
Re-assign a record to another folder (A.2.50)			M	M	
Copy an existing record to create a new one (A.2.51)	M				
Copy an existing record to allocate to an additional folder (i.e. a controlled copy) (A.2.52)	HD				
Create and declare an extract (A.2.56/57)			M	M	
Search for and display records, folders, classes and their metadata	M	M	M	M	M
Ability to define and maintain disposal rules (A.4.3/4)				M	M
Notify ERMS of external event occurrence (A.4.10)				M	M
Allocate disposal schedule to a class or folder (A.4.17)	X	M	M	M	M
Allocate disposal schedule to record_type (A.4.11)	X			M	M
Allocate schedule to specific record of record_type (A.4.20)			M	M	M
Re-allocate schedule to folder or class (A.4.21)	X	M	M	M	M
Place disposal hold (A.4.25)	X		M	M	M
Initiate and confirm disposal process (A.4.30)	X		M	M	M
Delete a record outside of disposal function (A.4.65)	X	X	X	X	M
Delete minimum metadata (A.4.72)	X	X	X	X	M
Add and maintain users (A.5.3)	X	X	X	X	M
Define Access control markings (A.5.6)	X	X	X	X	M
Maintain user profiles (A.5.16)	X	X	X	X	M
Define user roles (A.5.17)	X	X	X	X	M
Define and maintain access control groups (A.5.22)	X	X	X	X	M
Allocate allowable access controls (A.5.26) (A.5.7/8)	M		M	M	M
Modify audit trail data (A.6.5)	X	X	X	X	X
Configure audit rail tracking (A.6.6)	X	X	X	X	M
Run management reports (A.7.1)			M	M	M
Define pre-set metadata field values (A8.19)	X				HD
Configure unique identifier patterns (A.9.4)	X				HD
Specify back-up conditions (A.9.13)	X		X		HD
Restore system from back-up and forward build	X		X		HD

USER METADATA ELEMENTS

<i>Metadata element</i>	<i>M/D</i>	<i>Rep? Y/N</i>
USERNAME	M	N
Name	M	N
User rôle	M	Y
User business group access permission	M	Y
User protective marking security category	M	N
User descriptor category	M / O	Y

Note: Retention of 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 functional requirements, nor the metadata standard include this as part of the cross government core requirement.

ACCESS CONTROL MODEL

The access control model inherent in these functional requirements is consistent with that required by the Manual of Protective Security. 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 to 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 system, 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 general 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

Security categories

The standard hierarchy of levels is:

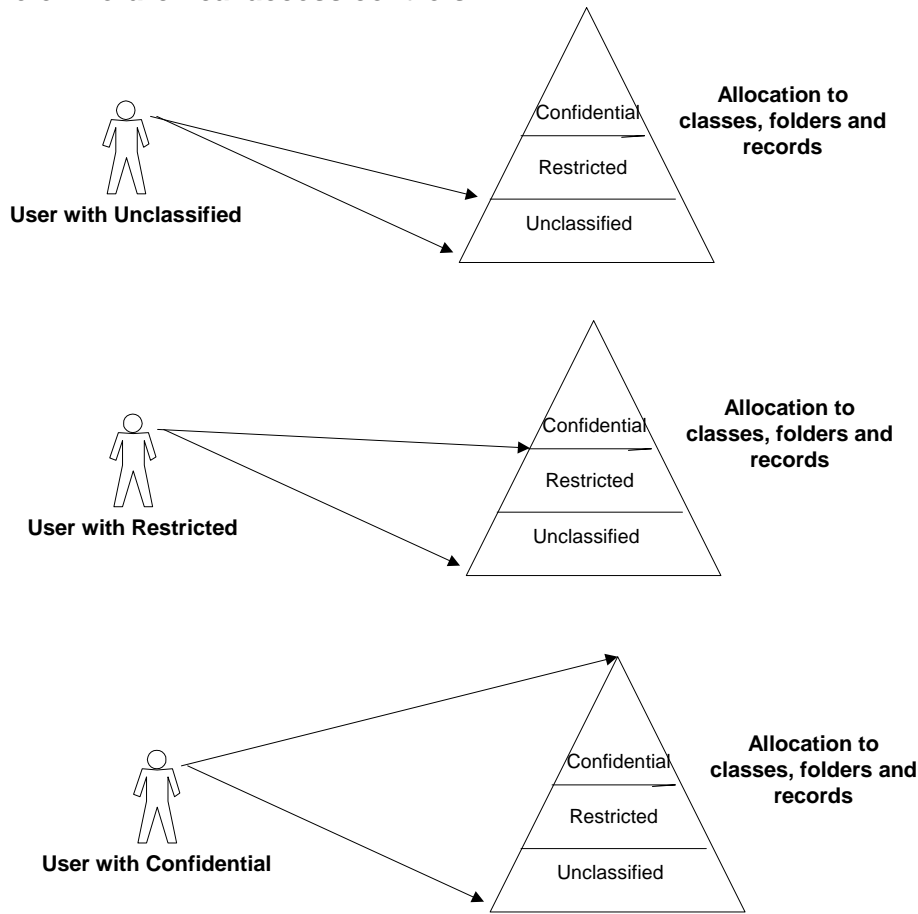
- Top Secret (highest level)
- Secret
- Confidential
- Restricted
- Unclassified (lowest level)

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

The majority of records are allocated the lowest level – Unclassified – and relatively few are allocated the highest level. A user to whom the highest level is allocated has the greatest breadth of access permissions. For example:

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

Example of hierarchical access controls



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 should 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.

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 ERM System – 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; Personnel staff.

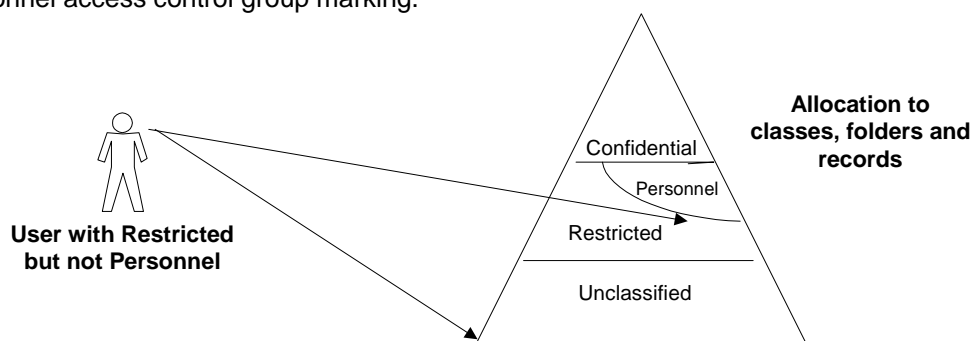
The group name can then be applied once, rather than listing each individual separately; but there is an overhead in maintaining up-to-date membership of a large number of groups. There is a balance to be struck between the advantage of easy application, and the cost of maintenance.

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.



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.

FLAT LISTING OF METADATA ELEMENTS

This section sets out a 'flat' listing of the metadata elements for:

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

which are identified by specific requirements in the Functional Requirements (2002) and the accompanying Metadata Standard [User metadata appears in the following section].

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

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.
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 folder².

² There are a number of metadata elements where population of the field is optional in the Metadata Standard but the presence of the functionality to capture it is phrased as a Mandatory in the Requirements. In those cases, the ability to support the capture of the metadata by the functionality is a mandatory functional requirement

Functional Requirements for Electronic Records Management Systems : Reference

6. The column headed *Source* indicates – for the record level only - whether the metadata standard **requires** this value to be captured automatically or from a user, or whether it **must** be inherited from a higher level of aggregation. Other metadata (including metadata at other levels) **may** be inherited where this is appropriate (e.g. for administrative convenience).

Class level metadata elements

<i>Ref</i>	<i>Metadata element</i>	<i>Obligation level</i>	<i>Rep? Y/N</i>
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	N
6.4	Date.Opened	Mandatory	N
6.5	Date.Closed	Mandatory if applicable	N
9.3	Relation.Parent object	Mandatory	Y
10.	Aggregation	Mandatory	N
17.1	Mandate.Authorising statute	Optional	Y
17.2	Mandate.Personal data acquisition purpose	Optional	N
17.3	Mandate.DPA exempt category (processing)	Optional	N

Folder level metadata elements

<i>Ref</i>	<i>Metadata element</i>	<i>Obligation level</i>	<i>Rep? Y/N</i>
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	N
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 ¹	Mandatory	Y

Functional Requirements for Electronic Records Management Systems : Reference

<i>Ref</i>	<i>Metadata element</i>	<i>Obligation level</i>	<i>Rep? Y/N</i>
9.3	Relation.Parent object	Mandatory	N
9.7	Relation.'See also' relational folder link(s)	Optional	Y
9.8	Relation.Hybrid paper folder relational link	Optional ³	N
10	Aggregation	Mandatory	N
12.1	Location.Home location	Mandatory	N
12.2	Location.Current location	Optional	N
13.1	Rights.Protective marking	Mandatory	N
13.2	Rights.Descriptor	Mandatory if applicable	Y
13.3	Rights.Protective marking expiry date	Optional	N
13.4	Rights.Custodian	Mandatory if applicable	N
13.5	Rights.Individual user access list	Mandatory	N
13.6	Rights.Group access list	Mandatory	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	Optional	N
13.10	Rights.DPA data subject access exemption	Optional	Y
13.11	Rights.EIR disclosability indicator	Optional	N
13.12	Rights.control.EIR exemption	Optional	Y
13.13	Rights.Fol disclosability indicator	Mandatory	N
13.14	Rights.Fol Exemption	Optional	N
13.15	Rights.Date of last FOI disclosability review	Optional	Y
13.16	Rights.Fol release details	Mandatory if applicable	Y
13.17	Rights.FOI release date	Mandatory if applicable	N
14.1	Disposal.Schedule identifier	Mandatory	N
14.2	Disposal.Disposal action	Mandatory	N
14.3	Disposal.Disposal time period	Mandatory	N
14.4	Disposal.Disposal event	Mandatory if applicable	N ⁴

³ *i.e. =part[s] at this level of aggregation. Minimum mandatory requirement if hybrid folder management offered.*

⁴ *A retention period which is either time-based or event-based, or both, will always be present.*

Functional Requirements for Electronic Records Management Systems : Reference

<i>Ref</i>	<i>Metadata element</i>	<i>Obligation level</i>	<i>Rep? Y/N</i>
14.5	Disposal.disposal external event occurrence	Mandatory if applicable	N
14.6	Disposal.Disposal (due/effective) date	Mandatory if applicable	N
14.7	Disposal.Disposal authorised by	Mandatory	N
14.8	Disposal.Disposal comment	Optional	Y
14.9	Disposal.Export destination	Mandatory if applicable	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	Disposal.Reviewer details	Optional	N
14.15	Disposal.Status (progress) of review	Optional	N
17.1	Mandate.Authorising statute	Optional	N
17.2	Mandate.Personal data acquisition purpose	Optional	N
17.3	Mandate.DPA exempt category (processing)	Optional	N

Part level metadata elements

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

Record level metadata elements

<i>Ref.</i>	<i>Metadata element</i>	<i>Obligation level</i>	<i>Rep? Y/N</i>	<i>Source</i>
1.1	Identifier.System ID	Mandatory	N	System
1.2	Identifier.Fileplan ID	Optional	N	System
2	Title	Mandatory	N	User
3	Subject	Optional	Y	User
4	Description	Optional	N	User
5	Creator	Mandatory	N	System
6.1	Date.Created	Mandatory	N	System

Functional Requirements for Electronic Records Management Systems : Reference

<i>Ref.</i>	<i>Metadata element</i>	<i>Obligation level</i>	<i>Rep? Y / N</i>	<i>Source</i>
6.2	Date.Acquired	Optional (Mandatory for email)	N	User (System for email)
6.3	Date.Declared	Mandatory	N	System
7	Addressee	Optional (Mandatory for email)	N	User (System for email)
8.1	Type.Record type	Mandatory where applicable	N	System
9.1	Relation.Copy[/Pointer?]	Mandatory where applicable	N	System (or user according to functionality available)
9.3	Relation.Parent object	Mandatory	N	System
9.4	Relation.Redaction/Extract	Mandatory if applicable	Y	System (or user according to functionality available)
9.5	Relation.Reason for redaction/extract	Mandatory if applicable	Y	User
9.6	Relation.Rendition	Mandatory if applicable	Y	System (or user according to functionality available)
9.7	Relation.'See also' relational links	Optional	Y	User
10.	Aggregation	Mandatory	N	System
11.	Language	Optional	N	User (default [ISO 639-2/B] Eng)
13.1	Rights.Protective marking	Mandatory	N	User ⁵
13.2	Rights.Descriptor	Mandatory where applicable	Y	User
13.3	Rights.Protective marking expiry date	Optional	N	User
13.4	Rights.Custodian	Optional	N	User
13.5	Rights.Individual user access list	Mandatory	N	User
13.6	Rights.Group access list	Mandatory	Y	User

⁵ This and the other sub-elements of Rights would often be expected to be inherited from the folder level, although this is not a mandatory requirement. Indeed the Functional requirements demand the ability to manage access at the record level.

Functional Requirements for Electronic Records Management Systems : Reference

<i>Ref.</i>	<i>Metadata element</i>	<i>Obligation level</i>	<i>Rep? Y/N</i>	<i>Source</i>
13.7	Rights.Previous protective marking(s)	Optional	Y	System
13.8	Rights.Previous protective marking(s) change date(s)	Optional	Y	System
13.9	Rights.Disclosability to DPA data subject	Optional	N	User
13.10	Rights.DPA data subject access exemption	Optional	N	User
13.11	Rights.EIR disclosability indicator	Optional	N	User
13.12	Rights.EIR exemption	Optional	N	User
13.13	Rights.Fol disclosability indicator	Mandatory	N	User ['Y'/'N' default 'Y']
13.14	Rights.Fol Exemption	Optional	N	User
13.15	Rights.Date of last FOI disclosability review	Optional	N	User
13.16	Rights.Fol release details	Mandatory if applicable	Y	User
13.17	Rights.FOI release date	Mandatory if applicable	N	User
14.1	Disposal.Schedule identifier	Mandatory	N	<i>Inherited</i>
14.2	Disposal.Disposal action	Mandatory	N	<i>Inherited</i>
14.3	Disposal.Disposal time period	Mandatory	N	<i>Inherited</i>
14.4	Disposal.Disposal event	Mandatory if applicable	N ⁶	<i>Inherited</i>
14.5	Disposal.disposal external event occurrence	Mandatory if applicable	N	<i>Inherited</i>
14.6	Disposal.Disposal (due/effective) date	Mandatory if applicable	N	<i>Inherited</i>
14.7	Disposal.Disposal authorised by	Mandatory	N	<i>Inherited</i>
14.8	Disposal.Disposal comment	Optional	Y	<i>Inherited</i>
14.9	Disposal.Export destination	Mandatory if applicable	N	<i>Inherited</i>

⁶ A retention period which is either time-based or event-based, or both, will always be present.

Functional Requirements for Electronic Records Management Systems : Reference

Ref.	Metadata element	Obligation level	Rep? Y/N	Source
14.10	Disposal.Export status	Optional	N	<i>Inherited</i>
14.11	Disposal.Review date	Optional	N	<i>Inherited</i>
14.12	Disposal.Review comment	Optional	N	<i>Inherited</i>
14.13	Disposal.Date of last review	Optional	N	<i>Inherited</i>
14.14	Reviewer details	Optional	N	<i>Inherited</i>
14.15	Status (progress) of review	Optional	N	<i>Inherited</i>
<u>15.</u>	<u>Digital signature (under investigation)</u>	=	=	=
17.1	Mandate.Authorising Statute	Optional	N	User
17.2	Mandate.Personal data acquisition purpose	Optional	N	User
17.3	Mandate.DPA exempt category (processing)	Optional	N	User

E-mail transmission data mapping⁷

Ref.	E-mail transmission data element	Electronic record metadata element	Source
2	Subject line ⇒	Title	User
5	E-mail sender name ⇒	Creator	System
6.1	Date / time of transmission ⇒	Date.Created	System
7	E-mail recipient(s) ⇒	Addressee	System
6.2	Date / time of e-mail receipt ⇒	Date.Acquired	System

Component level metadata elements

Ref.	Metadata element	Requirement	Obligation level	Rep? Y/N	Source
15.1	Preservation.Originating format	-	Optional ⁸	N	System

⁷ Email transmission mapping is not given sequential numbering in its own right in the flat list – see main record level table

⁸ 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 www.state.me.us/CIO/accessibility/software_policy.html

A program must provide keyboard access to all functions of the application. All actions required or available by the program must be available with keystrokes, i.e., keyboard equivalents for all mouse actions including but not limited to, buttons, scroll windows, text entry fields and pop-up menus.

A program must have a keyboard control sequence among all program controls and focal points. (e.g. using the tab key to navigate among edit fields, text boxes, buttons, and all other controls).

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 the timing parameter can be adjusted by an individual user.

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.

All icons 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.

For graphic text, system text drawing tools or other industry standard methods must be used so that screen reader software can interpret the image.

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

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 color settings system wide. Highlighting should also be Viewable with inverted colors.

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.

MAPPING OF FUNCTIONAL REQUIREMENTS

PROI Requirements 1999 and 2002, with MoReq and US DoD 5015.2 Standard Requirements

(US DoD 5015.2 Requirements mapping to be added)

Symbols key

** Highly Desirable (PRO 2002)

^ Desirable (PRO 1999)

* Desirable (PRO 2002)

∃ Desirable (MoReq)

PRO: Revised requirements	PRO: 1999	MoReq : 2001	DOD 5015.2 : 2002
Record Organisation			
Classification scheme / fileplan			
A.1.1	A.1.1	(3.1.1)	
A.1.2	A.1.2	3.1.2, (3.1.3)	
A.1.3	A.1.5	3.1.5	
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	-	-	
A.1.9	-	-	
** A.1.10	^ A.1.22	∃ 3.1.8	
* A.1.11	^ A.1.23	∃ 3.1.9	
<i>Class metadata</i>			
A.1.12	-	(3.2.1)	
A.1.13	-	-	
A.1.14	A.1.3	3.2.2	
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	-	-	
A.1.20	^ A.1.28	3.2.5	
A.1.21	-	∃ 12.1.11	
** A.1.22	-	-	
A.1.23	-	-	
** A.1.24	^ A.1.24	∃ 3.2.6	
<i>Folders</i>			
A.1.25	(A.1.2)	3.2.3	
** A.1.26	-	∃ 3.2.7	

Functional Requirements for Electronic Records Management Systems : Reference

PRO: Revised requirements	PRO: 1999	MoReq : 2001	DOD 5015.2 : 2002
** A.1.27	^ A.1.26	ᵛ 7.1.6	
A.1.28	-	3.2.9	
<i>Folder metadata</i>			
A.1.29	A.1.15	(3.2.1, 12.1.20)	
A.1.30	-		
A.1.31	-	12.1.2	
A.1.32	-	ᵛ 12.1.11	
** A.1.33	-	-	
A.1.34	-	-	
A.1.35	-	-	
A.1.36	(A.1.4)	3.2.5	
** A.1.37	^ A.1.24/25	ᵛ 3.2.8	
A.1.38	^ A.2.10	-	
<i>Folder management</i>			
A.1.39	A.1.6	3.2.4	
A.1.40	(A.1.6)	-	
A.1.41	A.1.10	3.4.7	
A.1.42	(A.1.10)	-	
A.1.43	-	(3.4.9)	
A.1.44	A.1.11	(3.3.6)	
A.1.45	(A.1.12)	-	
A.1.46	A.1.14	3.4.6	
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	-	ᵛ 3.4.5	
* A.1.51	^ A.1.29	ᵛ 3.4.11	
<i>Parts</i>			
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	ᵛ 3.4.8	
A.1.61	(A.1.8)	3.3.4	
A.1.62	-	-	

Functional Requirements for Electronic Records Management Systems : Reference

PRO: Revised requirements	PRO: 1999	MoReq : 2001	DOD 5015.2 : 2002
A.1.63	(A.1.9)	3.3.5	
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	
Capture and declaration			
Capture			
A.2.1	(A.2.1)	(6.1.1)	
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)	э 6.3.4	
A.2.6	A.2.7	-	
A.2.7	-	-	
A.2.8	A.2.6	6.1.13	
A.2.9	(A.2.6)	(6.3.2)	
A.2.10	-	э 6.4.2	
A.2.11	-	э 6.4.2	
** A.2.12	-	-	
<i>Declaration</i>			
A.2.13	A.2.2	(6.1.1)	
A.2.14	A.2.4	4.5.4	
A.2.15	A.2.3	(9.3.1)	
A.2.16	-	-	
A.2.17	(A.2.12)	э (6.1.6)	
** A.2.18	-	(10.8.4)	
A.2.19	A.2.16	6.1.8	
A.2.20	-	6.3.5	
A.2.21	A.1.16	э (6.1.5)	
** A.2.22		(3.4.13)	
** A.2.23	-	6.1.15	
A.2.24	(A.1.17)	-	
** A.2.25	^ A.2.31	э 6.1.11	
<i>Record types</i>			
A.2.26	-	-	
A.2.27	-	-	
A.2.28	-	-	
A.2.29	-	-	

Functional Requirements for Electronic Records Management Systems : Reference

PRO: Revised requirements	PRO: 1999	MoReq : 2001	DOD 5015.2 : 2002
<i>Record metadata</i>			
A.2.30	(A.2.8)	6.1.2	
A.2.31	-	-	
A.2.32	A.2.8	6.1.3	
A.2.33	A.2.11	↗ 12.1.22	
A.2.34	(A.2.11)	↗ 12.1.22	
* A.2.35	-	(12.1.9)	
A.2.36	-	↗ (8.1.10)	
* A.2.37	^ A.2.29	↗ (8.1.10)	
A.2.38	-		
A.2.39	A.2.12	12.1.23 -24	
A.2.40	-	-	
A.2.41	(A.2.13)	12.1.20	
A.2.42	(A.2.13)	9.3.8	
A.2.43	A.2.9	12.1.3/4/21	
A.2.44	A.2.14	6.1.7	
A.2.45	A.2.20	(6.1.4), 6.1.9	
A.2.46			
A.2.47	A.2.30	↗ 6.4.3	
A.2.48	A.2.15	(12.1.13)	
A.2.49	A.2.17	(7.1.1-3)	
<i>Move, copy extract and relate</i>			
A.2.50	A.1.13	3.4.2	
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	↗ 6.1.5	
** A.2.56	-	9.3.9	
** A.2.57	-	↗ 9.3.12	
** A.2.58	^ (A.2.27)	↗ 9.3.13	
A.2.59	-	-	
** A.2.60	-	9.3.11	
** A.2.61	^ (A.2.27)	↗ 8.1.26	
** A.2.62	-	4.3.6	
<i>Bulk import</i>			
A.2.63	(9)	6.2.1	
** A.2.64			
A.2.65	(9)	-	

Functional Requirements for Electronic Records Management Systems : Reference

PRO: Revised requirements	PRO: 1999	MoReq : 2001	DOD 5015.2 : 2002
A.2.66	(9)	6.2.1	
** A.2.67	(9)	6.2.2	
Search and Display			
A.3.1	(8)	8.1.1	
A.3.2	-	-	
A.3.3	A.1.21	3.1.7/8.1.13	
Searching			
A.3.4	A.1.20	(8.1.4), 8.1.6	
A.3.5	(8)	∃ 8.1.10	
A.3.6	-	8.1.5	
A.3.7	(8)	∃ 8.1.9	
A.3.8	-	(8.1.8)	
A.3.9	(8)	8.1.8	
A.3.10	-	8.1.7	
A.3.11	(8)	∃ 8.1.20	
** A.3.12	-	∃ (8.1.22)	
A.3.13	(8)	8.1.8, 8.1.11	
* A.3.14			
A.3.15	-	8.1.17	
A.3.16	A.1.18	8.1.15	
A.3.17	A.1.19	8.1.14	
A.3.18	B.4.23	8.1.28	
** A.3.19	-	-	
<i>Display</i>			
A.3.20	-	8.1.18	
A.3.21	A.2.21	∃ 8.2.3	
A.3.22	-	(4.4.3), 8.3.13	
A.3.23	-	-	
A.3.24	A.2.22	(8.2.1)	
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	
<i>Presentation</i>			
** A.3.29	-	-	
** A.3.30	-	-	
A.3.31	(A.3.38)	-	
** A.3.32	-	-	

Functional Requirements for Electronic Records Management Systems : Reference

PRO: Revised requirements	PRO: 1999	MoReq : 2001	DOD 5015.2 : 2002
Retention and disposal			
<i>Disposal: definition</i>			
A.4.1	^ (A.3.19)	5.1.3, 5.1.1	
A.4.2	-	(5.1.3)	
A.4.3	A.3.6	5.1.2	
A.4.4	(A.3.15)	(5.1.15)	
A.4.5	-	-	
A.4.6	-	-	
A.4.7	A.3.7-8	5.1.7	
A.4.8	A.3.9	5.1.12	
A.4.9	A.3.10	5.1.11	
A.4.10	A.3.11	5.1.11	
A.4.11	-	-	
A.4.12	A.3.13	5.1.10	
** A.4.13	-	ᄁ (5.1.5)	
<i>Disposal: scheduling</i>			
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	
** A.4.18	-	-	
** A.4.19	-	-	
A.4.20	(A.3.15)	5.1.16	
** A.4.22	-	-	
** A.4.23	-	-	
A.4.24	^ A.3.20	ᄁ 5.1.18	
A.4.25	-	-	
A.4.26	-	-	
A.4.27	-	-	
A.4.28	-	-	
<i>Disposal: execution</i>			
A.4.29	A.3.12	5.1.1	
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	
* A.4.33	-	-	
A.4.34	(A.3.14)	(5.1.13)	
A.4.35	-	-	
A.4.36	-	-	

Functional Requirements for Electronic Records Management Systems : Reference

PRO: Revised requirements	PRO: 1999	MoReq : 2001	DOD 5015.2 : 2002
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	-	-	
<i>Review</i>			
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			
<i>Export and transfer</i>			
A.4.50	A.3.25	5.3.1	
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)	⊃ (5.3.5)	
A.4.58	-	-	
** A.4.59	-	⊃ 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	-	
A.4.63	A.3.32	5.3.7	
<i>Destruction</i>			
A.4.64	(A.3.33)	5.2.7	
A.4.65	-	9.3.7	
A.4.66	-	-	
A.4.67	A.3.35/45	⊃ 5.3.13	
A.4.68	-	5.3.14	
** A.4.69	^ A.3.46	5.3.15-16	
** A.4.70	-	(5.3.15)	
** A.4.71	-	-	

Functional Requirements for Electronic Records Management Systems : Reference

PRO: Revised requirements	PRO: 1999	MoReq : 2001	DOD 5015.2 : 2002
** A.4.72	-	-	
A.4.73	-	9.3.7	
A.4.74	-	-	
Access control			
<i>Access to ERMS</i>			
A.5.1	-	(4.1.2)	
** A.5.2	-	-	
A.5.3	-	-	
** A.5.4	-	(4.1.2)	
<i>Access control markings</i>			
A.5.5	B.4.1	-	
A.5.6	B.4.26	(4.1.1)	
A.5.7	(B.4.4)	3 (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	
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	
<i>Roles</i>			
A.5.17	B.4.32	4.1.3	
A.5.18	B.4.33	-	
A.5.19	B.4.34	4.5.1	
A.5.20	B.4.36	-	
** A.5.21	-	-	
<i>Groups</i>			
A.5.22	(B.4.6)	4.1.4/6	
A.5.23	-	-	
A.5.24	-	(4.1.1), 9.11.7	
** A.5.25	-	(4.1.2)	
<i>Classes, folders, records</i>			
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	

Functional Requirements for Electronic Records Management Systems : Reference

PRO: Revised requirements	PRO: 1999	MoReq : 2001	DOD 5015.2 : 2002
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	-	-	
<i>Custodian</i>			
A.5.41	B.4.7	-	
A.5.42	B.4.11	-	
A.5.43	(B.4.13)	-	
A.5.44	B.4.13	-	
<i>Access control : execution</i>			
A.5.45	B.4.2	-	
A.5.46	B.4.20	4.6.8	
A.5.47	(B.4.9)	4.1.1	
A.5.48	(B.4.9)	4.1.1	
A.5.49	B.4.10	-	
A.5.50	(B.4.9)	(4.1.1)	
** A.5.51	^ B.4.15	4.1.9	
A.5.53	(B.4.23)	4.1.10	
<i>Privacy and opening</i>			
A.5.52	-	-	
<i>Audit</i>			
A.6.1	B.5.1	4.2.1	
A.6.2	B.5.1	4.2.4	
A.6.3	B.5.8	4.2.6	
A.6.4	B.5.2	4.2.2	
A.6.5	B.5.3	(4.2.1)	
** A.6.6	^ B.5.10	э 4.2.7	
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	

Functional Requirements for Electronic Records Management Systems : Reference

PRO: Revised requirements	PRO: 1999	MoReq : 2001	DOD 5015.2 : 2002
** A.6.12	B.5.6	4.2.9	
<i>Reporting</i>			
A.7.1	-	9.2.1	
** A.7.2	-	9.2.7, (5.2.2)	
A.7.3	-	9.2.4	
A.7.4	-	9.2.4	
A.7.5	-	э (9.2.3)	
A.7.6	-	-	
A.7.7	^ A.1.32	3.4.14	
A.7.8	A.2.33	(9.2.1)	
A.7.9	^ A.3.24, 16-17	5.2.1,8,11	
A.7.10	-	(9.2.1)	
A.7.11	-	(9.2.1)	
Usability			
A.8.1	(D.10.1)	11.1.4	
A.8.2	-	э (11.1.4)	
A.8.3	-	-	
A.8.4	-	-	
** A.8.5	(D.10.1)	э 11.1.2	
* A.8.6	^ B.4.35	-	
A.8.7	(D.10.1)	11.1.3	
A.8.8	-	(11.1.3)	
** 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	
* 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
A.8.20	-	э 11.1.13	
A.8.21	-	-	
A.8.22	-	э 11.1.14	
Design and Performance			
A.9.1	-	11.2.8	
<i>Integrity</i>			
A.9.2	-	(9.1.2)	

Functional Requirements for Electronic Records Management Systems : Reference

PRO: Revised requirements	PRO: 1999	MoReq : 2001	DOD 5015.2 : 2002
A.9.3	-	7.1.1	
** A.9.4	-	↗ 7.1.7	
A.9.5	-	(11.4.7)	
A.9.6	-	(11.4.7)	
<i>Interfaces</i> A.9.7	-	-	
** A.9.8	-	-	
* A.9.9	-	-	
* A.9.10	-	-	

PRO : 1999 Requirements which are not mapped to any new 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 new 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	

REFERENCES

UK legislation

Public Records Act 1958

Data Protection Act 1998

Freedom of Information Act 2000

Environmental Information Regulations 1992 (as amended 1998)

Relevant standards documents

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 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**

Public Record Office Publications (<http://pro.gov.uk/recordsmanagement>)

Data Protection Act 1998: A guide for records managers and archivists, PRO 2000

Management, appraisal and preservation of electronic records 2 vols., PRO, 1999

Manual of guidance on access to public records, PRO 2001

Office of the e-Envoy publications (<http://e-envoy.gov.uk>)

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

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 'MoREQ' specification**, 2001 accessed from <http://www.cornwell.co.uk/moreq>

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>

- END OF DOCUMENT -