

Functional Requirements

for

Electronic Records Management Systems

2 : Reference Document

November 1999

Electronic Records Management Systems

This Reference Document should be read in conjunction with the companion volume *Functional Requirements for Electronic Records Management Systems, 1: Statement of Requirements*. It is intended as a supporting document for these functional requirements, and should be read in the light of the primary document.

Contents

INTRODUCTION	5
1. GLOSSARY OF TERMS	7
2. RECORDS MANAGEMENT ENTITY-RELATIONSHIPS	11
COMMENTARY ON ENTITY-RELATIONSHIPS	12
3. ELECTRONIC FOLDER ENTITY LIFE HISTORY	15
ELECTRONIC FOLDER ENTITY LIFE HISTORY COMMENTARY	18
4. EXAMPLE DISPOSAL SCHEDULES	21
5. ELECTRONIC RECORD ENTITY LIFE HISTORY	23
ELECTRONIC RECORD ENTITY LIFE HISTORY COMMENTARY.....	24
6. SECURITY AND ACCESS MODELS	27
CONTROLLING ACCESS TO RECORDS AND FOLDERS.....	27
CONTROLLING ACCESS TO FUNCTIONS	32
7. BASELINE METADATA ELEMENTS ARISING FROM REQUIREMENTS	35
ELECTRONIC FOLDER METADATA ELEMENTS	36
ELECTRONIC PART METADATA ELEMENTS	37
ELECTRONIC RECORD METADATA ELEMENTS.....	37
E-MAIL TRANSMISSION DATA MAPPING	39
USER METADATA ELEMENTS	39

Introduction

Purpose of this document

In the field of electronic records management there is no universally agreed definition of some of the key terms, such as *record*, and varying usage of common terms such as *file*. To ensure that the accompanying functional requirements for electronic records management systems are unambiguous, it is essential that the meaning of these terms as they are used in these documents is clearly understood.

Consequently, these models have been developed to set out formal definitions and illustrations of key terms, *as they are used in these requirements*. This reference document is intended specifically to assist common understanding of the requirements document; it makes no attempt to address any wider purpose. Accordingly, these models and definitions represent the records management domain only partially, in order to illustrate particular concepts used in the accompanying Statement of Requirements.

This document should be used in conjunction with the main document detailing functional requirements, where further clarity is needed to understand a particular requirement. Where the reference document is cited in a numbered detailed requirement, the cited portion will form the explicit context of that requirement.

Structure of this document

This document consists of the following sections:

1. **Glossary:** an alphabetic listing which defines key terms as they are used throughout the functional requirements. For a good understanding of the requirements, it is important that the particular usage of the terms in this glossary is understood.
2. **Entity-relationship diagram:** this depicts some of the key terms, and the relationships between them, in graphical form.

Commentary on entity-relationship diagram: designed to accompany the diagram, this commentary explains some of its important implications and their underlying rationale.

3. **Electronic folder entity life history:** this models the evolution of an electronic folder from creation, through management and incremental addition of records, to final disposal by destruction or permanent preservation.

Electronic folder entity life history commentary: this commentary highlights some implications of the diagram and the underlying rationale.

4. **Example disposal schedules:** example disposal schedules, illustrating the type of schedules which an electronic records management system will be required to support.
5. **Electronic record entity life history:** this depicts in graphical form the evolution of an electronic record, from its creation as a document through its transformation into a record, to its eventual destruction or archival preservation.

Electronic record entity life history commentary: designed to accompany the diagram, this commentary explains some of its important implications and their underlying rationale.

6. **Security and access models:** this section illustrates the requirements for electronic folder and record access controls, including the application of protective markings as a means of controlling access to records and folders; and the requirements for control of access to functions within the system, according to the rôle to which a user is allocated.
7. **Baseline metadata arising from requirements:** a list of metadata elements for electronic folders, electronic parts, electronic records, and users which are specified in, or consequent on, the detailed functional requirements.

1. Glossary of terms

This glossary defines key terms used in the specification (i.e. in the functional requirements as well as in this document). Some definitions are closely adapted from the glossary in BSI DISC PD 0008; these are marked with an asterisk (*). Terms defined in the glossary are shown in italics.

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.*

Note: an audit trail generally consists of one or more lists, or a database which can be viewed in that form. The lists can be generated by a computer system (for computer system transactions) or manually (for manual activities).

classification (1)

A scheme which categorises *records* into thematic assemblies designed to preserve the context of the *records* relative to each other.

Note: this categorisation can be achieved by, for example, allocation to a named group, by assignment of index information from a thesaurus or by attribution of a functional record type.

classification (2)

A scheme of protective 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

cut-off

A fixed period, or recurring date, which defines the point in time at which an electronic folder part 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 are frozen and that it formally passes into corporate control and is thereby declared as a *record*.

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)

Information, stored on a physical medium, which can be interpreted in an application context.

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 data files.

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 fileplan

A schema which defines the *electronic folders* used – their naming principle, organisation and structure, and constituent parts.

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.

entry

Metadata which describes the location of *records* stored in *electronic folders*.

file

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

folder

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*, *paper folder* to refer to that specific type of folder.

hybrid folder

A set of related electronic and/or non-electronic *records*, physically stored partly in an electronic folder within the system and partly in a non-electronic folder (typically, a paper folder) outside the system.

instance

(of a *record*) A copy of a record to which some changes have been applied, to remove (or mask) but not to add to or meaningfully amend existing content. This term is not in general use and is employed here to avoid confusion with the term *version*. The process by which information is masked is sometimes known as redaction.

Note: the changes usually result from restrictions on disclosure of information. For example, a *record* may be made available only after individuals' names are removed; in this case, an *instance* of the record is created in which the names have been made illegible.

marker

Metadata which describes attributes of a non-electronic *record* or an *electronic record* stored externally to the system (e.g. on a CD-R).

paper folder

A device for holding paper documents including, among others, envelopes, box files, ring or other type of binder.* When used in the requirements, this term refers to information about a paper folder (i.e. metadata), which is used by the system to assist in the management of physical paper folders.

part (n)

A subdivision of an *electronic folder* or *paper folder*.

Note: the subdivisions are created to improve manageability of the folder.

permanent preservation

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

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 (called sub-markings in these requirements) taken from controlled lists, which indicate the access controls applicable to a record.

Note: see the separate description of protective markings for further definition.

record (n)

Some *document(s)* produced by an organisation in the course of its business, and retained by the organisation as evidence of its activities.* Where this term is used in isolation, it refers to both electronic and paper records.

Note: A record may consist of one or several *documents*, and so may be in any format. In addition to this content, it must also include contextual information and, if applicable, structural information.

review (n)

The examination of a *folder* or *part* (electronic or paper) to determine whether it should be destroyed, sent to an archive, or retained for a further review at a later date.

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-marking

One or more words which are part of a *protective marking*.

transfer

The process of exporting (usually groups of) complete electronic folders for permanent preservation in the Public Record Office, or other place of deposit.

version

(of a *document*) The state of a document at some point during its development.

Note: a version is usually one of the drafts of a *document*, or the final document. In some cases, however, finished documents exist in several versions, e.g. technical manuals. Note also that *records* cannot exist in more than one version.

2. Records management entity-relationships

This section presents an entity-relationship diagram showing, in simplified form, the most important entities concerned with documents, records and folders.

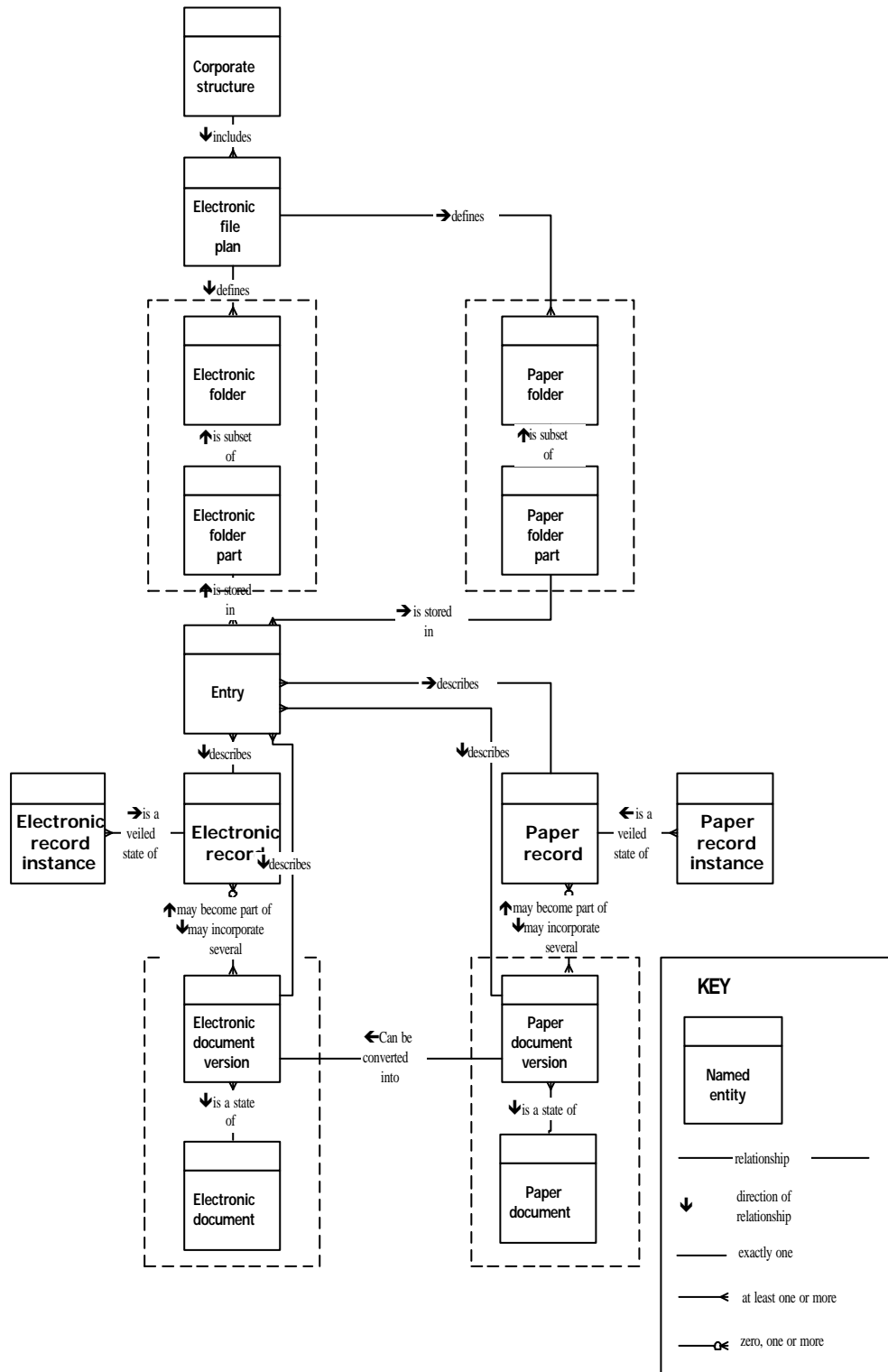


Fig. 2.1 : Partial model of records management

Commentary on entity-relationships

This diagram shows a wider context within which electronic records exist, and for purposes of clarity includes greater detail about the relationship between paper and electronic records and documents than is directly reflected in the functional requirements. It should be noted that these requirements do not focus strongly on the management of paper records in their own right; these are dealt with to the degree necessary for relating some continuing paper records to electronic records in the ERMS. Similarly, the requirements do not focus on the management of electronic documents which are not (yet) records.

The *relationships* in the diagram – the connecting lines – show the nature of the interactions between the entities; each relationship links two kinds of entity. For example, the relationship *defines* connects the entities *electronic file plan* and *folder*.

Note that the diagram is a simplified model of reality; it does not attempt to represent all possible relationships, rather the most significant ones for this application.

Key concepts

- a record can include one or more documents
- a document may appear in one or more records
- a document can have several versions, but a record cannot.

Entities

Corporate structure

The most fundamental entity is the *corporate structure*. Good records management practice requires that each organisation should set out a corporate policy for managing its records¹, and that it define the principles by which records will be kept. These collectively comprise the *corporate structure*. Because this structure contains information at a high level of abstraction, it does not generate any specific detailed requirements, and so is not mentioned in the requirements.

Electronic fileplan

Within this *corporate structure*, each organisation must have at least one fileplan. In the context of this partial model, the fileplan of interest is necessarily an *electronic fileplan*. This sets out the filing structure (typically consisting of folder hierarchy, folder numbers, names and descriptions) for a defined part of the organisation. The organisation may have several *electronic fileplans*, e.g. one per directorate or one per registry.

Folder

The *electronic fileplan* defines the existence of several *folders*. Each *folder* is either a *paper folder* (in hybrid systems) or an *electronic folder*.

A *paper folder* is the conventional container used to store physical documents and/or records (i.e. paper, audiotape, etc. rather than electronic). It may employ a ‘Treasury tag’, filing

¹ For further details, see *Management, appraisal and preservation of electronic records, vol. 1: Principles*, Public Record Office, 1999, p.18-28

prongs or some other means to hold records together. Note particularly that the term ‘file’ is avoided to prevent confusion with the IT usage of the same term.

An *electronic folder* is a collection of *electronic records* which have been associated together on the basis of some common theme or business function, and which will need to be managed and retrieved as a complete group.

Folder part

Folders are divided into *folder parts*, usually according to rules depending on size or number of *entries*. This practice originated with *paper folders*, in order to restrict them to a manageable size and weight. The practice is continued with *electronic folders*, to limit them to a manageable length for review, migration etc.

The terms *folder* and *folder part* are, in practice, used loosely or interchangeably: for example, a user will typically ask for “a *folder*” rather than (more accurately) for “a *folder part*,” and when a *folder* consists only of one *folder part*, it is not always labeled as the first part (often, the label is only applied when the second *folder part* is opened). Strictly speaking, all end users interact with *folder parts*, but this is often simplified to *folders*.

A pecked box has been drawn around *electronic folder part* and *electronic folder*. This is to reflect the reality that using the term *electronic folder part* instead of *electronic folder* is not helpful. Accordingly, the Requirements document and the remainder of this document use the term *electronic folder* or *folder* loosely, to mean *electronic folder part* in most cases.

Entry

Each *folder* contains *entries* which represent their contents. This term has been devised for this specification, and it is not in general use in records management.

An *entry* can be thought of in two ways:

- as a line in the *folder part* ‘contents list’
- as metadata for items held in the *folder part*

Each *entry* describes exactly one *electronic record* (or, optionally, one *paper record*). However, any of these records can be stored in several *folder parts* and thus can be described in several *entries*.

Record

At the heart of the system lies the most important entity, the *records*. These are the reason for the entire records management infrastructure, and form the record of the organisation’s activities.

Records are formed from *documents*. Each *record* can comprise one or several *documents*; and each *document* can appear in several *records*. A record cannot be changed in any way, without losing its integrity and value as a corporate record.

Record instance

It is sometime necessary to produce a sanitised copy of a *record*, for example to remove sensitive personal names. As *records* cannot themselves be modified this is referred to as producing a *record instance*; this applies to both electronic and physical *records*.

Document version and Document

Documents can exist in electronic or physical form.

Physical documents can be on paper, tape, film or any other medium. However, for simplicity, they are usually referred to as *paper documents* in the remainder of this specification.

Electronic documents are the digital equivalent of *paper documents*. Most commonly, they take the form of a word processing document or e-mail message, and can consist of several computer files: for example, a word processed report with embedded spreadsheet tables, or an intranet page with embedded graphics.

Documents can exist in several *document versions*. As with *file* and *file part*, there is some confusion over the distinction (because *documents* existing in only one version often are not allocated a version number).

A pecked box has been drawn around *electronic document* and *electronic document version*. This is to reflect the reality that using the term *electronic document version* instead of *electronic document* is not helpful. Accordingly, the Requirements document and the remainder of this Reference Document use the term *electronic document* loosely, to mean *electronic document version* in most cases.

3. 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.

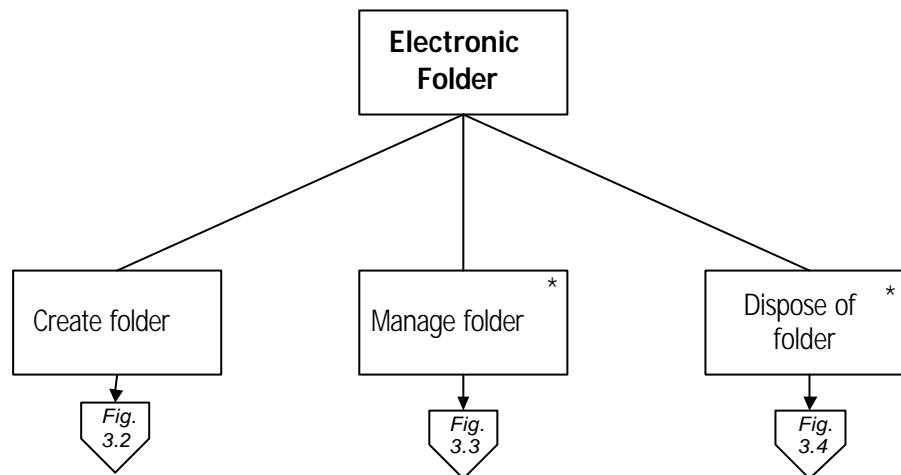


Fig. 3.1: **Electronic folder entity life history**

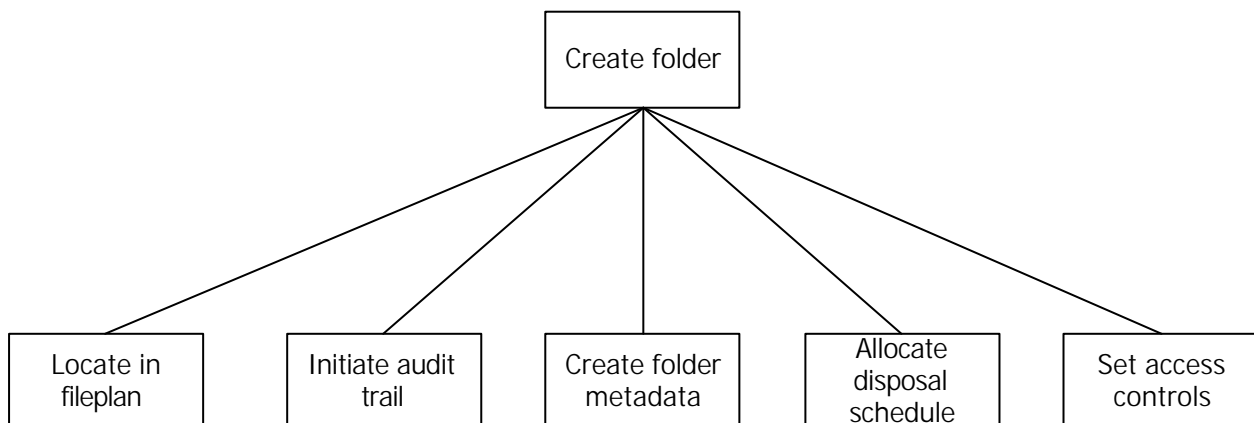


Fig. 3.2 : **Create electronic folder**

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

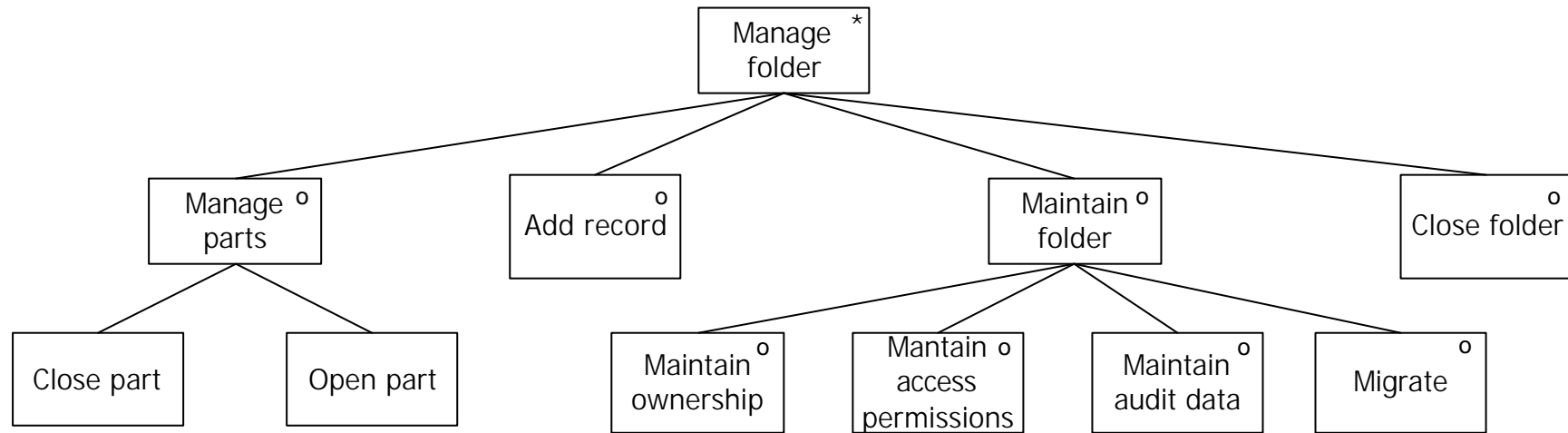


Fig. 3.3: **Manage electronic folder**

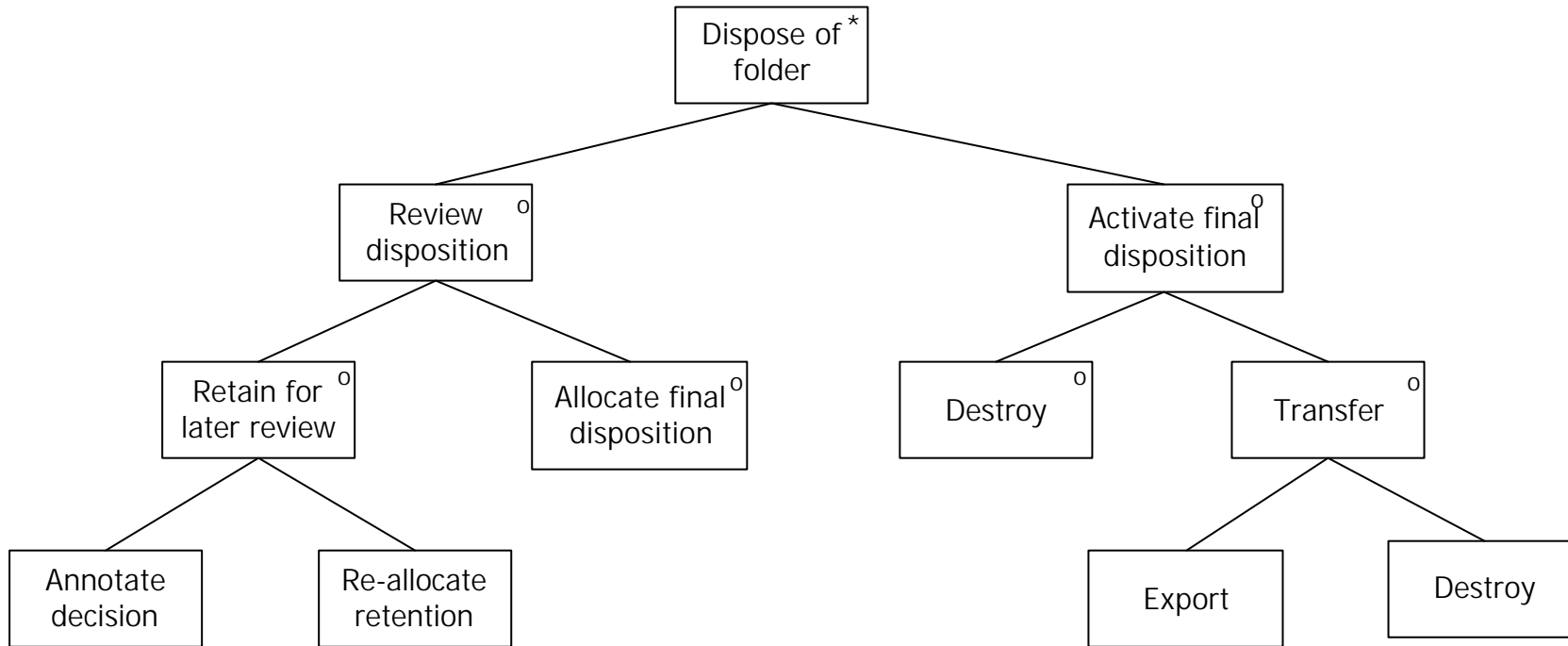


Fig. 3.4: **Dispose of electronic folder**

Electronic folder entity life history commentary

Key concepts

- a record is governed by the folder with which it is associated for purposes of management and disposal
- 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.

Destroy

The folder is destroyed; during this destruction, some of the metadata may 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

The folder is exported from the ERMS to another system (to a different department, or to the Public Record Office), including all records and associated metadata. Note that confirmation of successful export by the receiving organisation is required before destruction takes place.

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, and all its contents and metadata, is transferred to the Public Record Office or to another department or agency.

4. 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.

The list shown here is compiled from various fields of business and operation, and is given as illustrative examples, but not as definitive statements on these types of records. It is intended to show a range of retention periods and disposal actions which an ERMS will need to be capable of managing. It should be noted that a *Review* action may result in a decision to *Destroy*, to *Transfer for permanent preservation* or to *Retain* within the organisation for further review, at a later time.

Example schedules

<i>Type of records</i>	<i>Disposal</i>
General policy	Review 10 years after last addition
Correspondence : Local Authorities	Review 15 years after creation
Estate services test and statutory certificates	Retain in department for 30 years, followed by transfer for permanent preservation
Building Project Board minutes and papers	Review 25 years after issue of last paper
Project schedules	Destroy 10 years after completion of project
Claims and arbitration files	Review 16 years after creation
Maintenance manuals	Destroy when no longer required
Tender and evaluation board papers	Review 7 years after contract end
Asset registers	Destroy 6 years after asset, or last one in the register, is disposed of
Records relating to employees exposed to a listed biological agent	Destroy 10 years after last exposure
Above, where exposure may lead to a disease many years later	Destroy 40 years after last exposure
Health surveillance, including medical reports	Destroy 40 years from date of last entry
Reportable injuries, disease and dangerous occurrences	Destroy 3 years from date of report
Maintenance of control measures on control of lead at work	Destroy 5 years from date at which entry was made

5. 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.

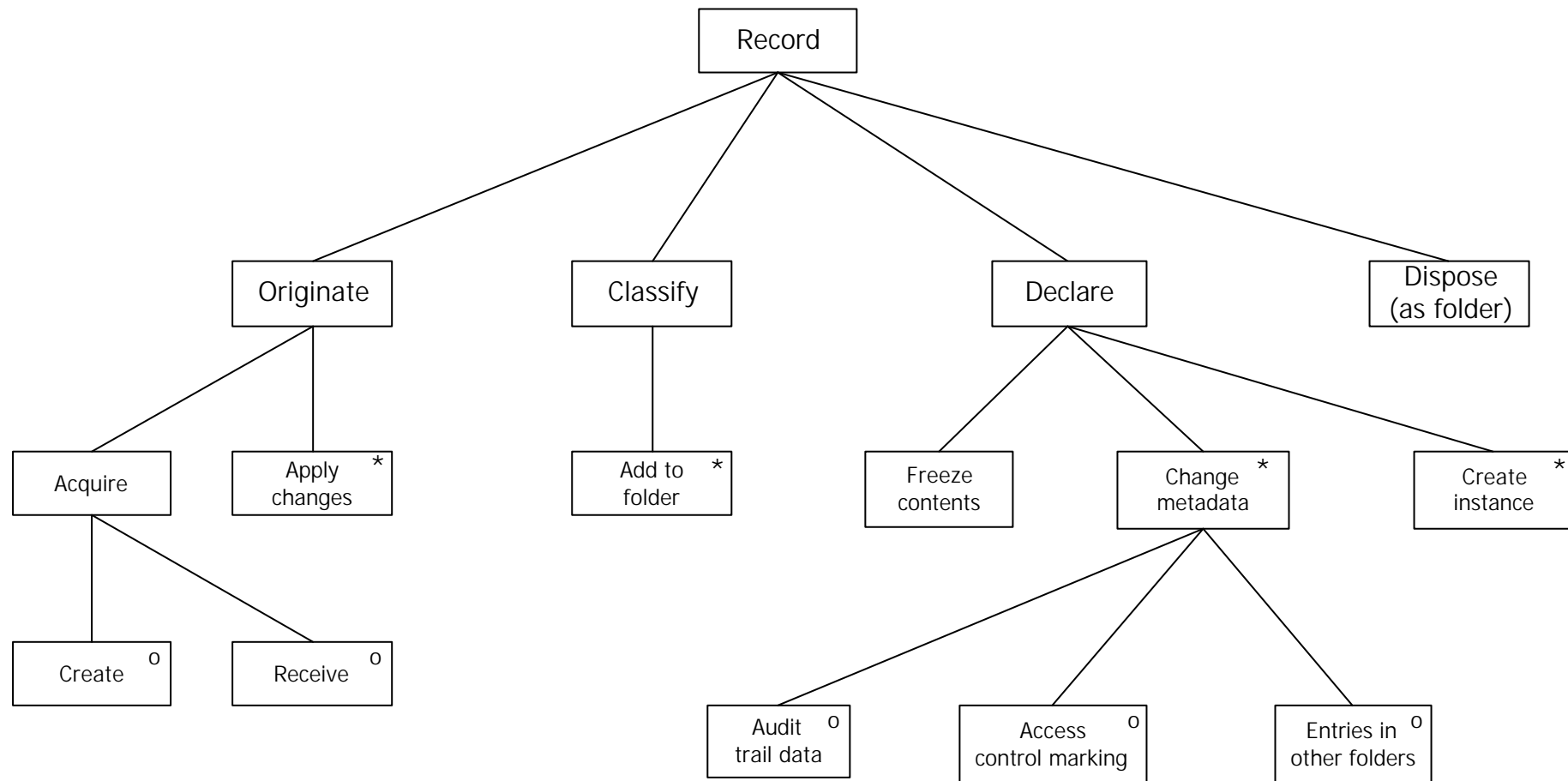


Fig. 5.1: Record life history

Electronic record entity life history commentary

Key concepts

- a version of a document may be declared to be a record at any time
- records 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.

Acquire in digital form

A record is originated as a document, by means of one of the two events below in the diagram structure.

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 trail data

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

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.

Create instance

A new instance of the record is created (e.g. a 'sanitised' copy). This is analogous to annotating the record, by removal (but not addition) of content. Note that the model does not

dictate whether such an instance does or does not become a record in its own right; but this would normally be the case.

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.

Disposal with 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 metadata may 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.

Freeze contents

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

Links to other folders

The record is allocated an entry in other folders, for example when it is sent to recipients who then declare a copy in their own folder.

Originate

Origination – the beginning of a document’s life – is one of the two events below it.

Receive

The document is received, usually by e-mail but possibly by some other means such as on a CD, or from another system, such as an image processing / scanning system.

6. Security and access models

This section deals with control of access to folders and records by means of protective markings and other access control groupings; and control of access to system functions by means of user rôles.

Controlling access to records and folders

Access is controlled by means of protective markings, allocation of business groups, and lists of named users.

Protective markings

Protective markings are a means of controlling access to specific folders, and specific records within folders, by allocating a marking (a word or phrase taken from a pre-defined list) to an individual folder or record. Folders and records marked in this way are only accessible to users who have been granted access permissions for the markings allocated to that folder or record. A general principle is that a user must have been granted permissions for *all* the protective markings (including sub-markings) which have been allocated to any specific folder or record, to be able successfully to gain access.

Security category

The protective marking scheme is made up of several sub-markings. The most fundamental sub-marking indicates a level of security 'classification'², hereafter called a security category. This is a word or phrase taken from a limited list, generally consisting of: UNCLASSIFIED, RESTRICTED, CONFIDENTIAL, SECRET, TOP SECRET. These terms are arranged in a hierarchy, with one end of the hierarchy indicating the highest level of protection, and the other end indicating that there is no restriction on access within government. Where there are no other access controls in force, a higher level security category encompasses access to lower level categories. Thus a user with access permission to folders or records marked *SECRET* will also have access permission, by virtue of this, to folders or records marked *CONFIDENTIAL* and *RESTRICTED*, unless some further restrictive access control has been allocated to those folders or records but not to that individual.

In addition to the security category sub-marking, there are several means by which access control can be qualified by a further sub-marking. These are called: *descriptors*; *caveats*; *codewords*; and *IDO markings*.

Descriptors

A descriptor is a word or phrase taken from a limited list, for example at present including: APPOINTMENTS; BUDGET; COMMERCIAL; CONTRACTS, etc. The list of users who will have access to records marked with a descriptor is unique to each record. For example, the term *CONTRACTS* will be used for widely differing actual contracts, and the list of users who are allowed access to folders or records dealing with one contract will differ from those allowed access to another, depending on its nature and business purpose. Therefore, a list of

² Note that the term 'classification' is used here to indicate a security category, and should not be confused with the use of the term to mean the organisation of records by classification to a folder within the corporate fileplan.

users for each of these terms cannot be pre-defined at a system-wide level.

A descriptor will be combined with a security classification category, for example as in: RESTRICTED: COMMERCIAL. More than one descriptor may be used.

Caveats

A *caveat* is a sub-marking, taken from a limited list, which broadly indicates nationalities. For example, the list at time of writing includes: UK EYES ONLY; CANUKUS EYES ONLY. The phrase indicates (simplifying slightly) the nationalities of users allowed to access a record or folder so marked; for example: CANUKUS EYES ONLY indicates 'Canadian, UK or US nationals only may access this document'. One or more caveats may also be allocated to an individual user; alternatively, a system may allocate one or more nationality(ies) to an individual user, from which access rights may be logically constructed by relating to caveats.

Codewords

A *codeword* is a sub-marking, which is a single word taken from a limited list. A codeword may be allocated to a folder, a record, and a user.

IDO markings

An IDO marking is a sub-marking, a word taken from a limited list, which indicates an International Defence Organisation marking. For example, the list at time of writing includes: NATO, WEU, etc. The phrase indicates (simplifying slightly) the origin of users allowed to access a record or folder so marked: for example: 'NATO' indicates 'NATO nationals only may access this document'; 'WEU' indicates 'Western European Union nationals only may access this document'. One or more IDO markings may also be allocated to an individual user; alternatively, a system may allocate one or more nationality(ies) to an individual user, from which access rights may be logically constructed by relating to IDO markings.

In principle, sub-markings may be combined, and will always apply with equal force in any allowed combination. However, some combinations may not be valid. For example, it might be defined that a *codeword* cannot be used with any security classification lower than *SECRET*.

Business groups

In addition to protective markings, there will be a need to control access to folders and records by the use of pre-defined business groups, such as project teams, members of committees, work groups, sections and branches. These groups are maintained lists of users who are allowed access to records and folders which have an identical access control marking.

Owner restrictions on access

The owner of a folder or record may wish to restrict access to a unique list of users, applied only to that folder or record. This list of users will be specific to the folder or record, and will be maintained by the owner (who may wish to add or remove users).

Publicly available records

The above access controls apply to the use of the system within the organisation in which it is implemented. Although, within the government context, there is no expectation of allowing direct public access to the records held in an ERMS, a copy of a record or folder may have been made publicly available by other means: for example, by publication on a website or in print. There will be a need to retain a knowledge of the fact that records or folders have been made public in this way, and the form in which this was done.

Schema of departmental records

Figure 6.1 overleaf maps a generic schema for records within a department or agency; specific differences will exist between individual departments.

Security marked material may include paper-based records, electronic records, and the indexes to these records. Unclassified records may include those which are held within the department at the lowest level of security category – *Unclassified* – but have not been opened to public availability; and records which *have* been opened to public availability by publication in some form.

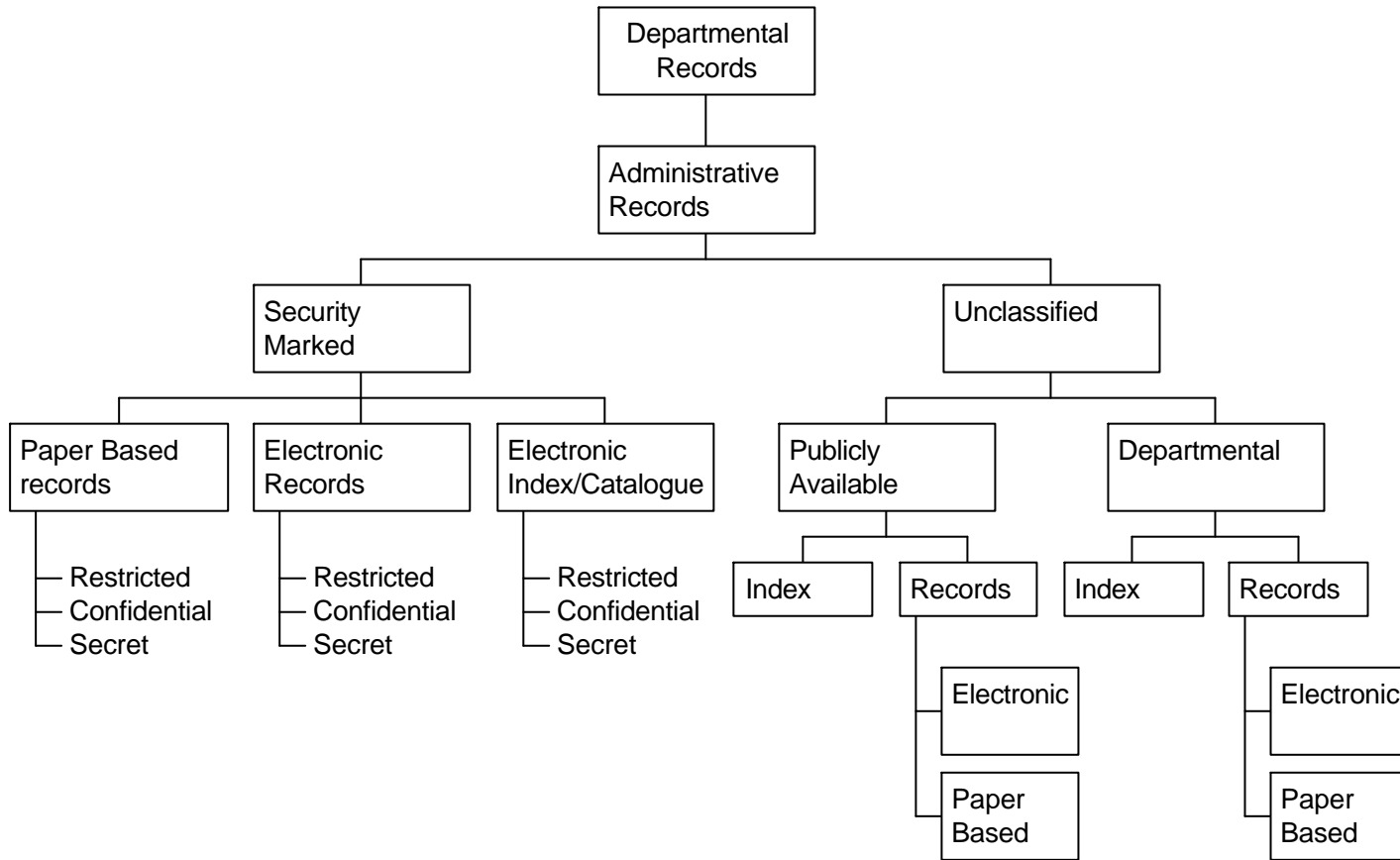


Fig. 6.1: Schema of departmental records

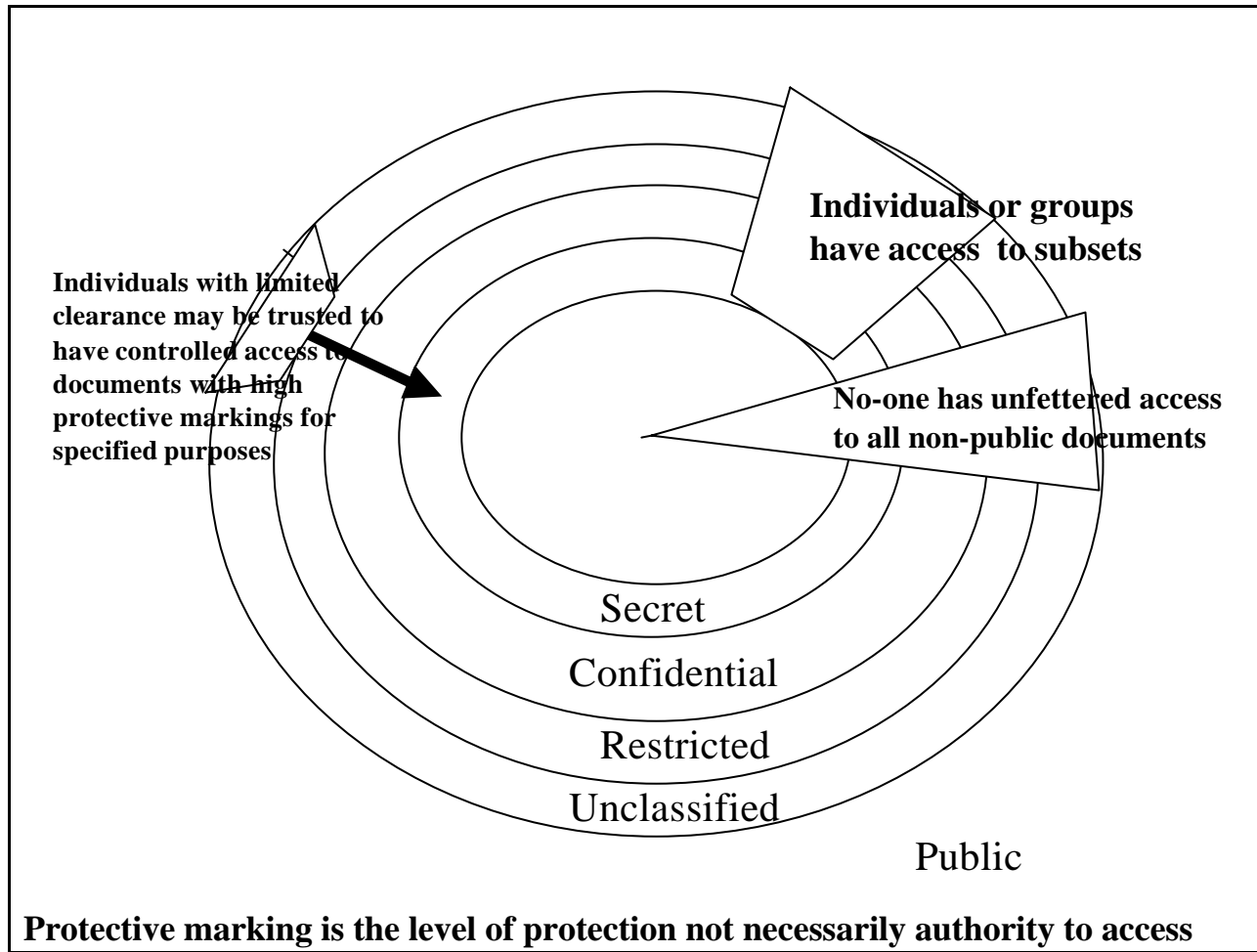


Fig. 6.2: Protective Marking and access limitations

Controlling access to functions

The requirements identify a number of functions to which access must be controlled by allocation of users to one or more user rôles and some functions where this would be desirable. This matrix shows those identified functions in relation to a set of generic user rôles. In some implementations, one or more of these rôles may be carried out by the same individual. Rôles relate to the ability to physically carry out functions within the system, and do not necessarily determine decision-making on policy or procedural questions.

In the table cells: *M = Identified in a Minimum Requirement*
 D = Identified in a Desirable Requirement
 Blank cell = Function not available in this rôle.

<i>Function</i>	End user	Reviewer	Records administrator	Records manager	Systems administrator
Create electronic document	M		M	M	M
Declare electronic record	M		M	M	M
Add electronic record to folder	M		M	M	M
Allocate access control markings	M ³		M ⁵	M ⁴	M ⁴
Allocate subject terms	D		D	D	D
Add electronic folders	M ⁵		M	M	M
Add electronic parts	M ⁵		M	M	M
Amend electronic folder metadata		M	M	M	M
Amend electronic record metadata	M ³		M	M	M
Open a closed part			M	M	M
Relocate a folder in fileplan			M ⁵	M	M
Relocate a record to another folder			M ⁵	M	M
Allocate a disposal schedule to an electronic folder			M ⁵	M	M
Confirm disposal action			M ⁵	M	M

³ For end users who are owners of that record or folder.

⁴ Where an owner cannot be determined, and subject to access controls.

⁵ May be determined by a policy decision within the organisation.

Export electronic folders as disposal action			M	M	M
Re-allocate a disposal schedule to an electronic folder		M		M	M
Display all disposal schedules				M	M
Amend a disposal schedule				M	M
Re-allocate a group of folders within the fileplan				M	M
View audit trail				M	M
Define fileplan/records reports				D	D
Allocate access permissions					M
Delete an electronic folder					M
Delete an electronic record					M
Configure metadata elements					M
Select system configuration					M
Maintain access control terms					M
Define user rôles and allocate to users					M
Configure audit trail					M
Define processing checks					D

Description of user rôles

The rôles described are generic rather than specific to every government organisation. They are presented as stereotypes, to assist with interpretation of this access matrix; specific task profiles will vary according to the size, nature and business needs of a department or agency.

End user

An end user is primarily concerned with creating, declaring and using records for business purposes. An organisation may allow an end user to create new folders as necessary, or may wish to restrict this ability to a records administrator.

Reviewer

A reviewer is typically an experienced end user who is no longer active in business operations (or a similar external person), rather than an internal member of records management staff. As such, a reviewer does not normally create and use current records, but is concerned with assessing the value and disposition of existing folders of records, as they enter the review process consequent on disposition instructions.

Records administrator

A records administrator is concerned with the day-to-day operation of electronic records management. This may include administration of the filing structure, providing assistance to end users in the classification and organisation of electronic records, and carrying out routine disposal, transfer and export activities. Some organisations may wish to restrict the functions which are available to records administrators (or only to some records administrators) to a greater degree than others.

Records manager

The records manager is concerned with developing and maintaining the infrastructure of the electronic records management system. This may include making decisions about the consistent allocation of disposal schedules across the fileplan, re-arranging the fileplan following business re-organisation, and resolving difficult and contradictory problem areas. The records manager will normally determine the appropriate operational configuration and selective behaviour of the ERMS, but will request a systems administrator to implement these decisions.

Systems administrator

A systems administrator is technically proficient in the configuration, operation and maintenance of the ERMS, and will have access to most (but possibly not all) system functions. The systems administrator will also be the single point of access at which the most drastic actions can be taken – deletion of folders and records as part of a ‘housekeeping’ activity – which will be subject to robust auditing procedures.

7. Baseline metadata elements arising from requirements

This section sets out the metadata elements for:

- electronic folders
- electronic parts
- electronic records
- users

which are identified by specific requirements in the Statement of Requirements for electronic records management systems.

The column headed *Ref.* contains a sequential reference number for each metadata element.

The column headed *Metadata element* contains the name for that metadata element.

The column headed *Requirement* contains the paragraph number for the most relevant requirement for that metadata element, as presented in the Statement of Requirements.

The column headed *M/D* indicates whether that requirement is a minimum (M) or desirable (D) requirement.

The column headed *Occ(urrence)* indicates the cardinality of the element as follows:

1 indicates that the metadata element occurs exactly once for each item (folder, part or record) to which it refers.

Example : There must be one, and only one, *electronic record unique identifier* for each electronic record in the ERMS.

1-n indicates that the metadata element occurs at least once for each item to which it refers, but may occur more than once.

Example : There must be at least one, but may be more than one, *entry* for each electronic record in the ERMS.

0-1 indicates that the metadata element may not always be present, but when it is present will occur once only. Note that this category includes metadata elements that will be required at some point in the lifecycle of the folder part or record (marked as **0-1** *), and metadata elements that may never be required for a specific item.

Example : An *electronic folder close date* 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.

0-n indicates that the metadata element may occur zero, one or many times for each item.

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.

Metadata elements which are typed as **1**, **1-n**, or **0-1** * are mandatory fields for metadata elements, since content must always be present at some point in the lifecycle of the item.

The column headed *S* (electronic records only) indicates an element which is system-generated.

Electronic folder metadata elements

<i>Ref.</i>	<i>Metadata element</i>	<i>Requirement</i>	<i>M/D</i>	<i>Occ.</i>	
01	Numerical reference code	A.1.3	M	0-1	
02	Folder title	A.1.3	M	1	
03	'Parent' electronic folder	A.1.2	M	1 ⁶	
04	'Child' electronic folder	A.1.2	M	0-n ⁷	} 1
05	Electronic part(s)	A.1.2	M	0-n ⁷	
06	Electronic folder open date	A.1.6	M	1	
07	Electronic folder close date	A.1.10	M	0-1 *	
08	Folder owner	B.4.7	M	0-1	
09	Folder subject term(s)	A.1.24	D	0-n	
10	Folder free-text description	A.1.28	D	0-1	
11	'See also' relational folder link(s)	A.1.29	D	0-n	
12	Folder business group access permission	B.4.8	M	0-n	
13	Folder username access list	B.4.10	M	0-n	
14	Folder protective marking security category	B.4.18	M	0-1	
15	Folder descriptor	B.4.22	M	0-n	
16	Time validity of folder access control marking	B.4.14	D	0-1	
17	Previous folder protective marking(s)	B.4.12	M	0-n	
18	Previous folder protective marking(s) change date(s)	B.4.12	M	0-n	
19	Folder codeword(s)	B.4.30	D/M ⁸	0-n	
20	Folder caveat(s) (Nationalities) ⁹	B.4.31	D/M	0-n	
21	Folder IDO marking(s) (Nationalities) ⁹	B.4.31	D/M	0-n	
22	Retention period – time period	A.3.7	M	0-1 ¹⁰	

⁶ Identifies higher level in fileplan hierarchy – at highest folder level, this will be the root level.

⁷ *Either* folder(s) *or* part(s) will always be present in folder metadata.

⁸ Minimum requirement if *further protective marking requirements* offered.

⁹ See explanation of caveats/IDO markings at p.28.

¹⁰ A retention period which is *either* time-based *or* event-based, *or* both, will always be present.

BASELINE METADATA

<i>Ref.</i>	<i>Metadata element</i>	<i>Requirement</i>	<i>M/D</i>	<i>Occ.</i>		
23	Retention period – event	A.3.7	M	0-1 ¹⁰	}	1 *
24	Retention period – occurrence of event	A.3.11	M	0-1		
25	Disposition instructions	A.3.13	M	1		
26	Review comment	A.3.21	D	0-1		
27	Status (progress) of review	A.3.22	D	0-1		
28	Reviewer details	A.3.22	D	0-1		
29	Export destination organisation	A.3.25	M	0-1		
30	Status (progress) of transfer	A.3.22	D	0-1		
31	Folder Freedom of Information release details	B.4.5	M	0-1		
32	Hybrid paper folder relational link	B.6.8	D/M ¹¹	0-1		
33	Folder user-defined metadata element(s)	A.3.42	D	0-n		

Electronic part metadata elements

<i>Ref.</i>	<i>Metadata element</i>	<i>Requirement</i>	<i>M/D</i>	<i>Occ.</i>
34	'Parent' electronic folder	A.1.3	M	1
35	Electronic part open date	A.1.8	M	1
36	Electronic part close date	A.1.8	M	0-1 *
37	Cut-off	A.1.30	D	0-1

Electronic record metadata elements

<i>Ref.</i>	<i>Metadata element</i>	<i>Requirement</i>	<i>M/D</i>	<i>Occ.</i>	<i>S</i>
38	Electronic record unique identifier	A.2.17	M	1	S
39	Document title	A.2.18	M	1	

* Items 22-28 are a repeating group to store related historical disposal/ review instructions

¹¹ Minimum requirement if *hybrid folder management* offered.

<i>Ref.</i>	<i>Metadata element</i>	<i>Requirement</i>	<i>M/D</i>	<i>Occ.</i>	<i>S</i>
40	Author / Originator	A.2.11	M	1	S
41	Record owner	B.4.7	M	0-1	
42	Date / time of record creation	A.2.11	M	1	S
43	Date / time of declaration	A.2.14	M	1	S
44	Entry(ies)	A.1.16	M	1-n	
45	Sequence number(s)	A.2.19	M	1-n ¹²	S
46	Circulation list	A.2.20	M	0-1	S
47	Physical record type	A.2.11	M	1	S
48	Logical record type	A.2.28	D	0-1	S
49	Record subject term(s)	A.2.29	D	0-1	
50	Record FoI release details	B.4.5	M	0-1	
51	Link between <i>Instance</i> and <i>Originating record</i>	A.2.27	D	0-1	S
52	Record business group access permission	B.4.8	M	0-1	
53	Record username access list	B.4.10	M	0-1	
54	Record protective marking security category	B.4.18	M	0-1	
55	Record descriptor	B.4.22	M	0-n	
56	Previous record protective marking(s)	B.4.12	M	0-n	
57	Previous folder protective marking(s) change date(s)	B.4.12	M	0-n	
58	Time validity of record access control marking	B.4.14	D	0-1	
59	Record codeword(s)	B.4.30	D/M	0-n	
60	Record caveat(s) (Nationalities) ⁹	B.4.31	D/M	0-n	
61	Record IDO marking(s) (Nationalities) ⁹	B.4.31	D/M	0-n	
62	Electronic signature authentication	B.5.13	D/M	0-1	
63	Certification authority	B.5.14	D/M	0-1	
64	User-defined metadata elements	A.2.10	M	0-1	

¹² Exactly one sequence number per entry in each different electronic folder, relating the sequence number to the relevant entry.

E-mail transmission data mapping

<i>Ref.</i>	<i>E-mail transmission data element</i>	<i>Electronic record metadata element</i>	<i>Req. no.</i>	<i>S</i>
40	E-mail sender name ⇒	Author / Originator	A.2.20	S
46	E-mail recipient(s) ⇒	Circulation list	A.2.20	S
42	Date / time of transmission ⇒	Date / time of record creation	A.2.20	S
39	Subject line ⇒	Document title	A.2.20	
65	Date / time of e-mail receipt ⇒	Date / time of e-mail receipt	A.2.20	S

User metadata elements

<i>Ref.</i>	<i>Metadata element</i>	<i>Requirement</i>	<i>M/D</i>	<i>Occ.</i>
66	Username	B.4.32	M	1
67	Name	B.4.32	M	1
68	User rôle	B.4.32	M	1-n
69	User business group access permission	B.4.8	M	0-n
70	User protective marking security category	B.4.19	M	0-n
71	User codeword(s)	B.4.30	D/M	0-n
72	User caveat(s) (Nationalities) ⁹	B.4.31	D/M	0-n
73	User IDO marking(s) (Nationalities) ⁹	B.4.31	D/M	0-n