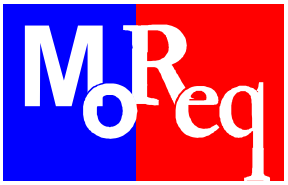
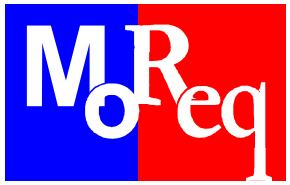


MODEL REQUIREMENTS FOR
THE MANAGEMENT OF ELECTRONIC RECORDS

MoReq SPECIFICATION

This specification has been prepared for
the IDA Programme
of the European Commission
by Cornwell Affiliates plc.

March 2001



MODEL REQUIREMENTS FOR
THE MANAGEMENT OF ELECTRONIC RECORDS

MoReq SPECIFICATION

This specification is available in electronic form at the following urls:

- http://cornwell.co.uk/moreq
- http://www.dlmforum.eu.org
- http://www.ISPO.cec.be/ida

March 2001

CONTENTS

1 INTRODUCTION

1.1 Background

The need for a comprehensive specification of requirements for electronic records management was first articulated by the DLM-Forum[1] in 1996, as one of the ten action points arising from its meeting. Subsequently, the European Commission Enterprise DG's Interchange of Data between Administrations (IDA) programme commissioned the development of this model specification.

Following an open competition in 1999, work on this specification started in 2000 and was concluded in early 2001. Development was carried out by a small team of specialist consultants from Cornwell Affiliates plc, supported by a guiding team of experts drawn from several countries, and validation organisations from both the private and public sectors.

Annex 2 contains further detail on the methodology used.

1.2 Purpose and Scope of this Specification

This specification describes Model Requirements for the Management of Electronic Record (MoReq). It focuses mainly on the functional requirements for the management of electronic records by an Electronic Records Management System (ERMS).

This specification is written to be equally applicable to public and private sector organisations which wish to introduce ERMS, or which wish to assess the ERMS capability they currently have in place.

While the specification focuses on functional requirements, it recognises that non-functional attributes are central to the success of an ERMS, as with any information system. However, these non-functional attributes vary enormously between environments. Accordingly, they are identified but described only in outline.

Other closely-related requirements, such as document management and the electronic management of physical records (e.g. paper files and microfilm) are also addressed, but in less detail. For example, the specification includes guidelines on the requirements for managing physical records; but it does not include all the detailed functionality associated with tracking physical locations, bar coding, etc.

---

1 DLM is an acronym for the French "Données Lisibles par Machine," in English: "machine-readable data." The DLM-Forum is based on the conclusions of the European Council (94/C 235/03) of 17 June 1994 concerning greater cooperation in the field of archives.

Related issues such as digitisation and other means of creating electronic records are outside the scope of this specification. Similarly, it makes no attempt to cover practical implementation of an ERMS.

This specification is written with the assumption that ERMS users include not only Administrators or Archivists, but also general office and operational staff who use ERMS as part of their everyday work while creating, receiving and retrieving records.

As this specification contains "model" requirements, it is designed to be entirely generic. It does not consider any platform-specific or sector-specific issues. Because it is modular, user communities can add to it additional functionality specific to their own business requirements (see section 1.6 and Annex 3 for guidance on using and customising this specification).

1.3 What is an ERMS?

The management of electronic records is complex, requiring a large range of functionality to be implemented well. Clearly, a system to meet these needs – an ERMS – requires specialised software. This software may consist of a specialist package, a number of integrated packages, custom-designed software or some combination; and in all cases, there will be a need for complementary manual procedures and management policies. The nature of an ERMS will vary from organisation to organisation. This specification makes no assumption about the nature of individual ERMS solutions. Users of this specification will need to determine how the functionality of an ERMS can be implemented to meet their requirements.

1.4 For What can this Specification be Used?

The MoReq specification is intended to be used:

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

- **by potential users of outsourced record management services:** as an aid in specifying the services to be procured.

The specification is written with an emphasis on usability. Throughout, the intention has been to develop a specification which is useful in practice.

1.5 Emphasis and Limitations of this Specification

The MoReq specification is designed explicitly with pragmatism and usability in mind. It is primarily intended to serve as a practical tool in helping organisations meet their business needs for the management of both computer-based and paper-based records. While its development has taken traditional archival science and records management disciplines into account, these have been interpreted in a manner appropriate to electronic environments. Thus, MoReq was developed with the needs of managers of both electronic and physical records in mind.

The requirements embodied in this MoReq specification should, if implemented, result in a system which will manage electronic records with the desired levels of confidence and integrity, by combining both the advantages of electronic ways of working with classical records management theory. Examples of this pragmatic approach include the incorporation of requirements for document management, workflow, metadata and other related technologies.

As explained in the scope, this specification attempts to cover a wide range of requirements - for different countries, in different industries and with different types of records. The wide scope is intentional; but it leads to a significant limitation, namely that this single specification cannot represent a requirement which precisely maps onto existing requirements without modification. Different countries have their differing traditions, views and regulatory demands for managing records. In some cases these will have to be taken into account when applying this Model Requirements Specification, especially when using it to specify a new system.

Also this work does not cover the practical aspects of the management of records. Intentionally, the specification addresses only the capabilities required for the management of electronic records by computer software. The specification avoids discussion of records management philosophy, archival theory, decision taking, management control etc.; these issues are well covered in other literature, some of which is listed in Annex 1. As a particular example, the specification mentions in several places that certain functions must be limited to an Administrator. This is not to say that Administrators have to take policy decisions, merely that they must be the only users empowered by the organisation to execute them through the ERMS.

Finally, this specification is intentionally user-centric; it uses, as far as possible, the type of terminology commonly used by those working with electronic records. For example, the specification describes electronic files as “containing” records, for

ease of understanding, even though these files strictly do not contain anything. See section 2.2 for further details.

1.6 Using this Specification

The requirements in this specification are intended to serve as a model. They are not prescriptive for all possible ERMS implementations; some requirements will not apply in some environments. Different business sectors, different scales, different organisation types and other factors will also introduce additional specific requirements. This specification must therefore be customised before use.

This specification has been prepared so that it can be used in paper or electronic form. It has been prepared using Microsoft Word 97 and Word 2000. Use in electronic form has a number of benefits; details are given in Annex 3.

1.7 Organisation of this Specification

The specification is organised into chapters which are divided into sections.

The next chapter provides an overview of some of the key requirements, starting with terminology which is central to this specification.

Chapters 3 to 11 contain the ERMS requirements in detail. Each chapter contains a logical grouping of functional requirements. However, given the nature of the subject matter there is inevitably some overlap between chapters.

Each requirement is presented in a standard format, as illustrated below.

The requirements are presented in the form of tables, with one requirement per table row. This is illustrated below.

Ref.	**Requirement**
13.1.1	The ERMS must provide …

NUMBER REQUIREMENT

Each requirement bears a number, and each is expressed in natural language.

Chapter 12 identifies the metadata elements which are needed to meet these requirements, relating them to the requirements.

Chapter 13 contains a formal reference model of ERMS as understood in this specification. This model can be used to understand key aspects of the specification, such as formal definitions of terms (e.g. file, volume, level) and the relationships which exist between them (e.g. “what can be stored in an electronic file?”).

The Annexes contains details of reference documents, administrative and other information.

1.8 Mandatory and Desirable Requirements

In this specification,

- the word “must” indicates that a requirement is likely to be considered mandatory in most ERMS implementations;
- the word “should” indicates that a requirement is likely to be considered desirable in most ERMS implementations.

1.9 Comments on this Specification

While correspondence cannot be entered into, comments and observations on this specification can be sent to:

dlm-forum@cec.eu.int

2 OVERVIEW OF ERMS REQUIREMENTS

This chapter starts by defining some key terms (section 2.1). This is followed by a narrative description of some key concepts (section 2.2), and an entity-relationship diagram which shows the model on which this specification is based (section 2.3).

2.1 Key Terminology

This specification requires certain terms to have precise meanings. Wherever possible, the meanings align with common usage, or usage generally agreed within the records management community. All the terms are defined in the Glossary (section 13.1); selected key definitions from the Glossary are reproduced here for ease of reference.

Terms in *italics* are defined in the Glossary.

capture

Registration, *classification*, addition of *metadata* and storage of a *record* in a system that manages *records*.

class

(in this specification only) The portion of a hierarchy represented by a line running from any point in the classification scheme hierarchy to all the files below it.

Note: this can correspond, in classical terminology, to a "primary class", "group" or "series" (or sub-class, sub-group, sub-series etc.) at any level in the classification scheme.

classification (verb)

Systematic identification and arrangement of business activities and/or *records* into categories according to logically structured conventions, methods, and procedural rules represented in a classification scheme.

Source: ISO 15489 (draft international standard; see Annex 1 reference [9]).

classification scheme

See classification.

Source: definition of "Classification System" in ISO 15489 (draft international standard; see Annex 1 reference [9]).

Note: a classification scheme is often represented as a hierarchy.

document (noun)

Recorded information or object which can be treated as a unit.

Source: ISO 15489 (draft international standard; see Annex 1 reference [9]).

Note: a document may be on paper, microform, magnetic or any 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 objects.

Note: documents differ from *records* in several important respects. See *record*.

electronic file

A set of related *electronic records*.

Source: PRO Functional Specification of "electronic file" (Annex 1 reference [2]).

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

electronic record

A *record* which is in *electronic* form.

Note: it can be in electronic form as a result of having been created by application software or as a result of digitisation, e.g. by scanning paper or microform.

ERMS

Electronic Record Management System.

Note: ERMS differ from *EDMS* in several important respects. See section 10.3 for more details.

metadata

(in the context of records management) Structured or semi-structured information which enables the creation, management and use of records through time and within and across domains in which they are created.

Source: Archiving Metadata Forum working definition (http://www.archiefschool.nl/amf).

Note: the distinction between data and its metadata can be unclear. For example, it is usually clear that the essential indexing data for a record (title, date etc.) is part of that record's metadata. However, the audit trail for a record, or the retention schedule for a record, can validly be considered to be either data or metadata, depending on the context. Different types of metadata can be defined, for example, for indexing, for preservation, for rendering etc. These details of metadata usage are beyond the scope of the MoReq specification.

record (noun)

Document(s) produced or received by a person or organisation in the course of business, and retained by that person or organisation.

Source: adapted from PRO Functional Specification (Annex 1 reference [2]).

Note: local national definitions may also apply.

Note: a record may incorporate one or several *documents* (e.g. when one document has attachments), and may be on any medium in any format. In addition to the content of the document(s), it should include contextual information and, if applicable, structural information (i.e.

information which describes the components of the record). A key feature of a record is that it cannot be changed.

volume

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

Source: definition of "part" in PRO Functional Specification (Annex 1 reference [2]).

Note: the subdivisions are created to improve manageability of the file contents by creating units which are not too large to manage successfully. The subdivisions are mechanical (e.g. based on number of records or ranges of numbers or time spans) rather than intellectual.

2.2 Key Concepts

The key concepts required to understand this specification are:

- record and electronic record;
- electronic file and volume;
- classification scheme;
- class;
- ERMS;
- capturing records;
- users roles.

Record and Electronic Record

The DLM Forum Guidelines (Annex 1 reference [6] section 2.4) suggest that records can be viewed as consisting of:

- content;
- structure;
- context;
- presentation.

The content is present in one or more physical and/or electronic documents which convey the message of the record. These are stored in such a way as to allow future users to understand them and their context. This implies that a record contains, in addition to the content of its document(s), information about the document's context and structure. The presentation depends on a combination of the records contents, structure and (in the case of electronic records) the software used to render it.

In the world of physical records, the vast majority of records are on paper and are included in files, physically constituted of one or more volumes of records inserted within paper folders. Procedural controls should prevent users from changing the records, or their positions within the file.

Similar concepts apply to electronic records. A record is constituted of one or more electronic documents. These documents can be word processing documents, e-mail messages, spreadsheets, moving or still images, audio files or any other type of digital object. The documents become records when they are set aside, that is, "captured" into the ERMS. Upon capture, the records are "classified", that is they are assigned codes corresponding to the classification scheme class to which they belong, allowing the ERMS to manage them.

Electronic File and Volume

Paper records are accumulated in paper files, contained in paper folders. The paper files are aggregated into a structure, or classification scheme. In an ERMS electronic records can be managed as if they are accumulated in electronic files and stored in electronic folders. Strictly, electronic files and folders need not have a real existence; they are virtual, in the sense that they do not really "contain" anything; in fact they consist of the metadata attributes of the records assigned to them. Further, in many cases, there need be no real distinction in the electronic system between file and folder. However, these details are not generally visible to ERMS users; ERMS application software allows users to view and manage folders as if as if they physically contained the documents logically assigned to the files. This user-centred view is carried forward into this specification. The rest of this specification therefore describes electronic files as "containing" records, for ease of understanding. Note however that while this specification provides functional requirements for the management of electronic files, it does not prescribe the manner in which the concept of electronic files is implemented.

In some cases, files are divided "mechanically" into file volumes, according to predetermined conventions. The term "mechanically" implies simple adherence to such conventions, which are not based on the intellectual content of the files, but on size, number of records contained in them, or time spans. This practice originated with paper files, in order to restrict them to a manageable size and weight. It can be continued with electronic files, to limit them to a manageable length for appraisal, transfer, or other management purpose.

While the distinction between files and file volumes is clear, the implications are less clear. This is because the implications of choosing to divide files into volumes vary according to implementation needs. The variation arises as:

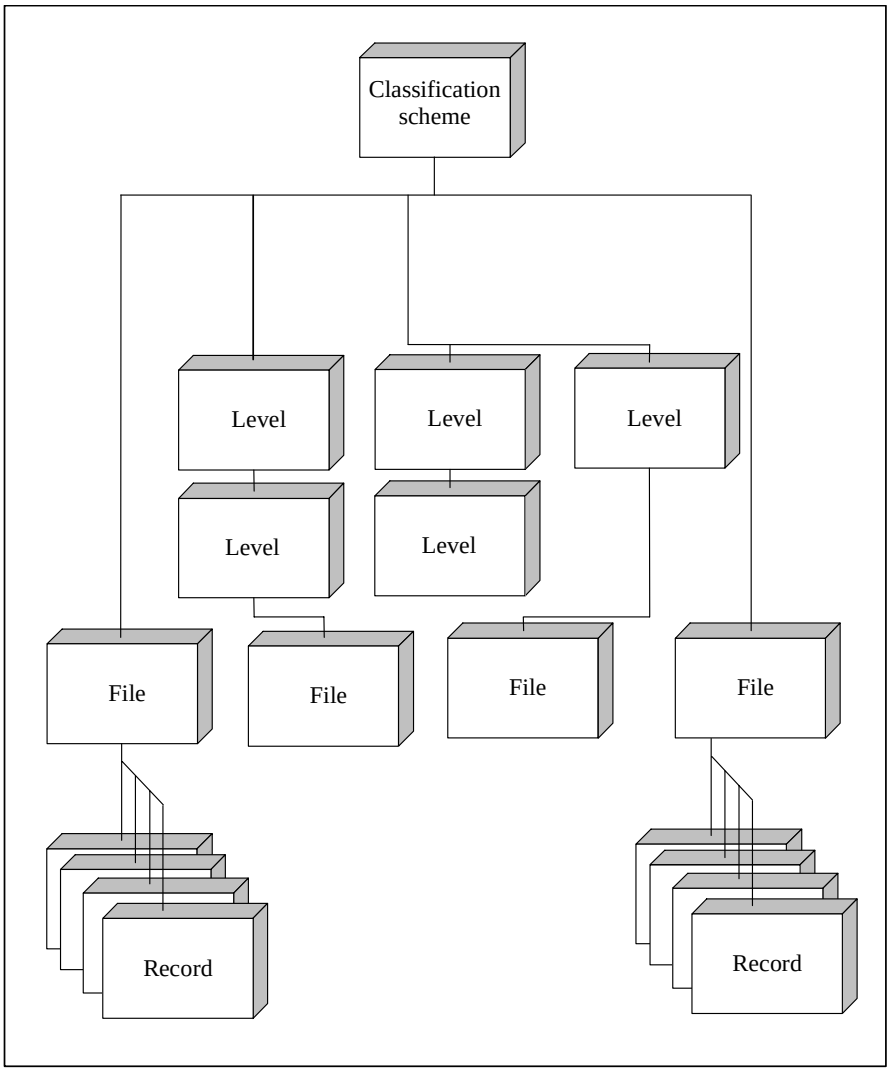
- some files are closed within a limited time, and so the unit used for management purposes is the file (even though a file may consist of several volumes). Examples are a file of a specific small procurement, or a file of one project;

- some files have an unlimited life span (or nearly unlimited life span), and so the unit used for management purposes is the volume. Examples are a file of records about a geographic region, or a file dealing with a subject which is not sensitive to time, such as some policies, or an invoice file where a new volume is started every year.

Classification Scheme

Records management aggregates files in a structured manner, and good practice dictates that this structure should reflect business functions. The representation of this aggregation is referred to as a "classification scheme". The classification scheme is commonly a hierarchy, though it may be supported by a thesaurus and may not be hierarchic. The remainder of this specification focuses on the hierarchical view.

Just as files appear to exist even though they are really no more than aggregations of records, so higher levels of the classification scheme hierarchy seem to exist, though they are no more than aggregations of files and/or lower levels. As with files, this specification states requirements for the hierarchy without mandating the manner in which it is implemented.



Files can appear at any level of the hierarchy. This is illustrated in the preceding figure, which is adapted from ISAD(G) (Annex 1 reference [7]).

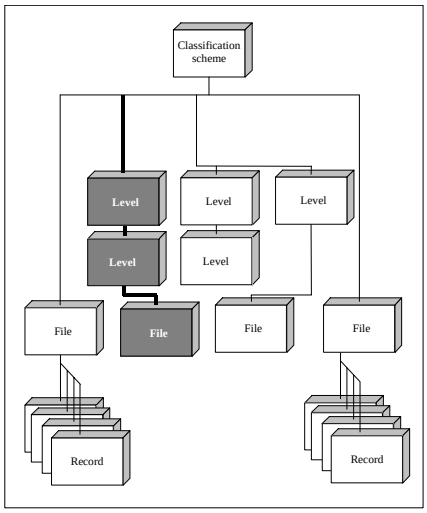
Note that this figure is intended only to show selected possible relationships between levels, files and records. It does not show all possible levels or all possible arrangements.

Class

This specification uses the term "class" to describe the portion of a hierarchy represented by a line running from any point of the hierarchy to all the files below it. The term class therefore corresponds to a "group" or "series" (or sub-group, sub-series etc.) in some texts.

In visual terms, a class of a hierarchy corresponds to a branch of a tree. A class may thus contain other classes, just as a series contains sub-series and sub-sub-

series. The shaded boxes and thick lines in the diagram to the right are one example of a class.



This specification makes no attempt to define how a classification scheme should be prepared; this is dealt with in other literature, for example the UBC-MAS work (Annex 1 reference [8]).

Electronic Record Management System (ERMS)

An ERMS is primarily an application for managing electronic records, though it may also be used to manage physical records. The emphasis of this specification is firmly on the management of electronic records.

An ERMS is often closely integrated with an Electronic Document Management System. Technically, an ERMS manages records, while an EDMS manages documents (which are not records). However, especially when used to support day-to-day working, it can be difficult to separate their functionality. This is explored further in section 10.3 which deals with Document Management issues.

Capturing Records

Documents made or received in the course of business become records when they are set aside, that is, "captured" into the ERMS. During capture, the records are "classified", that is they are assigned codes corresponding to the class to which they belong, allowing the ERMS to manage them; and they are also assigned a unique identifier.

In many cases, documents that are set aside, or captured, become records by being bound to a business process, for example as happens in a workflow. For example, when an invoice is raised it should automatically cause a record to be captured. In other cases there may be a policy that every document relating to a business matter must become a record, even if it does not formally participate in a business process. In yet other circumstances however, the process of capture will be initiated selectively by a user. Determination of which documents should be captured into a records system should be based on an analysis of the regulatory environment, business and accountability requirements and the risk of not capturing the records. An example is a memorandum in an organisation which deals with policy issues; the organisation may define that only memoranda deemed to be significant will become records (i.e. insignificant memoranda, such as those relating to meeting arrangements, will generally not form records). This specification is intended to cater for any of these scenarios. In other words, this MoReq specification describes an office system for general use, not simply a

records management system for particular kinds of application or for the exclusive use of Archivists or Administrators.

User Roles

This specification identifies two kinds of user:

"user" .....any person who is authorised to have access to the ERMS application. In practice, this means persons who make, receive, review and/or use records, and those who administer the ERMS.

"Administrator" .....a user who manages the records stored in the ERMS, and the ERMS itself together with its databases.

In practice, most organisations will have more than one person in these roles; and many organisations will define further roles. See section 13.4 for more detail.

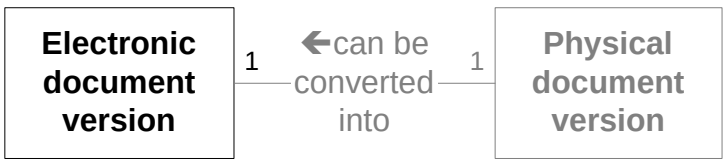
2.3 Entity-Relationship Model

This section contains an entity-relationship model which can be used as an aid to understanding the specification. Section 13.3 contains a narrative explanation.

An important aspect of this diagram is that it does not represent actual structures stored in the ERMS. It represents a view of the metadata associated with records. An ERMS uses this metadata to manage the records as if the structure shown in the diagram actually existed. See section 2.2 for further explanation of this point.

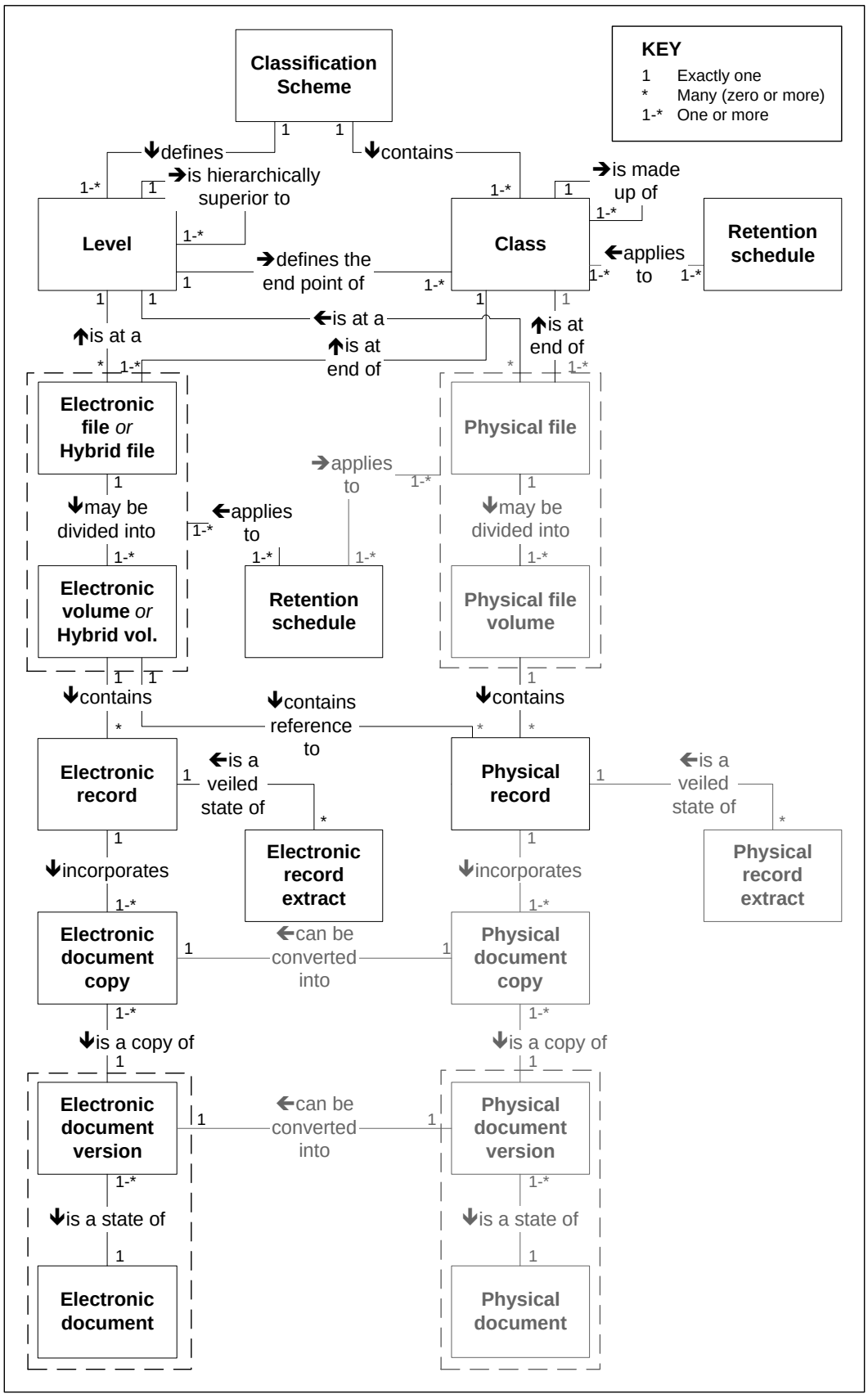
The relationships between files, volumes, records and other entities are depicted more rigorously in the following entity-relationship diagram. This is a formal representation of selected structures which comprise an ERMS.

In the diagram, entities – files, records and so on – are represented by rectangles. The lines connecting them represent the relationships between the entities. Each relationship is described by text in the middle of the line; and this should be read in the direction of the arrow. Each end of the relationship has a number which represents the number of occurrences (strictly, the cardinality); the numbers are explained in the key. So, for example, the following extract:



means "One physical document version can be converted into one electronic document version" (note the direction of the relationship arrow).

Note that the entity Class is related to itself by the relationship “is made up of”. This recursive relationship describes, in formal terms, the hierarchy of folders, in which a Class may contain other Class. Similarly, each Level may be hierarchically superior to other Levels.


KEY
1 Exactly one
* Many (zero or more)
1-* One or more
Classification Scheme
defines
contains
is hierarchically superior to
is made up of
Level
Class
Retention schedule
defines the end point of
applies to
is at a
is at end of
Electronic file or Hybrid file
Physical file
applies to
may be divided into
Electronic volume or Hybrid vol.
Retention schedule
Physical file volume
contains
contains reference to
Electronic record
is a veiled state of
Physical record
Electronic record extract
Physical record extract
incorporates
Electronic document copy
can be converted into
Physical document copy
is a copy of
Electronic document version
Physical document version
is a state of
Electronic document
Physical document

3 CLASSIFICATION SCHEME

A classification scheme lies at the heart of any ERMS, as described in detail in section 2.2. It defines the way in which the electronic records will be organised into electronic files, and the relationships between the files.

This chapter first lists requirements for setting up the classification scheme in section 3.1. It then lists requirements relating to classes and files (section 3.2) and volumes (section 3.3). The final section (3.4) lists requirements associated with maintenance of the classification scheme.

3.1 Configuring the Classification Scheme

Ref.	Requirement
3.1.1	The ERMS must support and be compatible with the organisation's classification scheme.
3.1.2	The ERMS must be able to support a classification scheme which can represent files as being organised in a hierarchy with a minimum of three levels. *Three levels are suggested here as a minimum; more levels will be needed in some environments.*
3.1.3	The ERMS should not limit the number of levels in the classification scheme hierarchy.
3.1.4	The ERMS must allow the naming mechanism(s) to be defined at configuration time.
3.1.5	The ERMS must support the initial construction of a classification scheme at configuration time in readiness for the capture or importation of electronic records.
3.1.6	The ERMS must allow Administrators to add new classes at any point within any class, so long as files are not stored at that point. *Note that this can be at any level.*
3.1.7	Where the ERMS is designed to employ a graphical user interface, it must support browsing and graphical navigation of the files and classification scheme structure; and the selection, retrieval and display of electronic files and their contents through this mechanism.
3.1.8	The ERMS should support the definition and simultaneous use of multiple classification schemes. *This may be required, for example, following the merger of two organisations. It is not intended for routine use.*

Ref.	Requirement
3.1.9	The ERMS should support a distributed classification scheme which can be maintained across a network of electronic record repositories.

3.2 Classes and Files

This section lists requirements which apply to classes and files.

Ref.	Requirement
3.2.1	The ERMS must support metadata for files and classes in the classification scheme; and after a record has been captured the ERMS must restrict the ability to add to or amend its metadata to Administrators. *Metadata requirements are described in chapter 12.*
3.2.2	The ERMS must provide at least two naming mechanisms for electronic files and classes in the classification scheme: • a mechanism for allocating a structured numeric or alphanumeric reference code (i.e. an identifier which is unique within the classification scheme – see chapter 7) to each electronic file; • a mechanism to allocate a textual file title for each electronic file. It must be possible to apply both identifiers separately or together in the same application.
3.2.3	The ERMS must allow Administrators to add (open) files at the lowest level of any class in the classification scheme. *Note that the lowest levels of all classes need not all be at the same level.*
3.2.4	The ERMS must record the date of opening of a new class or file within the file's metadata.
3.2.5	Whenever a new class or file is opened, the ERMS must automatically include in its metadata those attributes which derive from its position in the classification scheme (e.g. name, classification code). *For example, if a "Correspondence" file is in a hierarchical path:* *Regional plan development : Public consultation : Correspondence* *and the Administrator adds a new file named "Formal Objections" at the same level as the "Correspondence" file then it must automatically inherit the prefix "Regional plan development : Public consultation."*
3.2.6	The ERMS should support an optional class and file naming mechanism that is based on controlled vocabulary terms and relationships drawn from a ISO 2788-compliant or ISO 5964-compliant thesaurus and the linking of the thesaurus to the classification scheme.

Ref.	Requirement
3.2.7	The ERMS should support an optional class and file naming mechanism which includes names (e.g. persons' names) and/or dates (e.g. dates of birth) as file names, including validation of the names against a list. *This requirement is appropriate for transaction processing environments.*
3.2.8	The ERMS should support the allocation of controlled vocabulary terms compliant to ISO 2788 or ISO 5964 as descriptive class or file metadata subject terms, in addition to the other requirements in this section.
3.2.9	The ERMS must not impose any practical limit on the number of classes or files which can be defined.
3.2.10	The ERMS must allow the automatic creation and maintenance of a list, or repertory, of files.

3.3 Volumes

This section includes requirements relating to the use of volumes, which are typically used to subdivide files which might otherwise be unmanageably large.

Ref.	Requirement
3.3.1	The ERMS must allow Administrators to add (in other words, to open) electronic volumes to any electronic file which is not closed.
3.3.2	The ERMS must record the date of opening of a new volume in the volume's metadata.
3.3.3	Whenever a new volume is opened, the ERMS must automatically include in its metadata those attributes of its parent file's metadata which are common (e.g. name, classification code).
3.3.4	The ERMS must support the concept of open and closed electronic file volumes, as follows: • only the most recently created volume within a file can be open; • all other volumes within that file must be closed (subject to temporary exceptions required by 3.3.6). *Note that the records in a volume can be accessed regardless of whether the volume is open or closed.*
3.3.5	The ERMS must prevent the user from adding electronic records to a closed volume (subject to the exceptions required by 3.3.6).

Ref.	Requirement
3.3.6	The ERMS must allow an Administrator to re-open a previously closed volume temporarily for the addition of records, and subsequently to close that volume again. *This facility is intended to be used to rectify user error, e.g. if a volume was closed unintentionally.*

3.4 Maintaining the Classification Scheme

Ref.	Requirement
3.4.1	The ERMS must allow an electronic file and its volumes, or a complete class of the hierarchy, to be relocated to a different position in the classification scheme, and must ensure that all electronic records already allocated remain allocated to the file(s) and volume(s) being relocated. *This facility is intended for exceptional circumstances only, such as organisational mergers or other re-organisation, or to correct clerical errors. This requirement must be read together with 3.4.3, 3.4.4 and 3.4.5.*
3.4.2	The ERMS must allow an electronic record to be re-classified to a different electronic file volume. *This facility is intended for exceptional circumstances only, such as to correct clerical errors. This requirement must be read together with 3.4.3, 3.4.4 and 3.4.5.*
3.4.3	The ERMS must restrict to Administrators the ability to move classification scheme classes, files, volumes and records.
3.4.4	When any classes, files, volumes or records are reclassified the ERMS must keep a clear trace of their status prior to the reclassification, so that their entire history can be determined easily. *At a minimum, this must be stored in the audit trail. It may be desirable to record it elsewhere, e.g. in the metadata of the object(s) being moved.*
3.4.5	When any classes, files, volumes and records are reclassified the ERMS should allow the Administrator to enter the reason for the reclassification.
3.4.6	The ERMS must prevent the deletion of an electronic file or any part of its contents at all times, with the exceptions of: • destruction in accordance with a retention schedule – see chapter 5; • deletion by an Administrator as part of an audited procedure – see 9.3.
3.4.7	The ERMS must allow an electronic file to be closed by a specific Administrator procedure, and must restrict this function to an Administrator.

Ref.	Requirement
3.4.8	The ERMS should be able to close an electronic file volume automatically on fulfilment of specified criteria to be defined at configuration, including at least: • volumes delineated by an annual cut-off date; for example, the end of the calendar year, financial year or other defined annual cycle; • the passage of time since a specified event; for example, the most recent addition of an electronic record to that volume; • the number of electronic records which a volume contains. *Other criteria may be desirable in particular circumstances, for example when the size of the volume reaches the storage capacity of a removable disc.*
3.4.9	The ERMS must record the date of closing of a volume with the volume's metadata.
3.4.10	The ERMS must not allow any volume which has been temporarily re-opened (as in 3.3.6) to remain open after the Administrator who opened it has logged off.
3.4.11	The ERMS should allow users to create cross-references (that is, "see also" type links) between related files.
3.4.12	The ERMS must maintain internal integrity (relational integrity or otherwise) at all times, regardless of: • maintenance activities; • other user actions; • failure of system components. *In other words, it must be impossible for a situation to arise where any user action or any software failure results in an inconsistency within the ERMS or its database.*
3.4.13	The ERMS should support the ability to create multiple entries for an electronic record, in several electronic files, without physical duplication of the electronic record. *In other words, it should use pointers when capturing more than one record based on the same document.*
3.4.14	The ERMS should provide reporting tools for the provision of statistics to the Administrator on aspects of activity within the classification scheme, including the numbers of electronic files, volumes or records created, closed or deleted within a given period.

4 CONTROLS AND SECURITY

This chapter brings together requirements for a wide range of controls which relate to the security of the records.

Organisations must be able to control who is permitted to access records and in what circumstances, as records may contain personal, commercial or operationally sensitive data. The restrictions on access may also need to be applied to external users. For example, in some countries where freedom of information legislation permits access to selected public records, customers may wish to view records. Requirements for these controls are listed in section 4.1.

Any access to records, and all other activities involving them and related documents or data may also need to be stored in the audit trail to ensure legal admissibility and to assist in data recovery. Requirements for these audit trail controls are listed in section 4.2.

Security of records also includes the ability to protect them from system failure by means of backup, and the ability to recover the records from backups. These requirements are listed in section 4.3.

For various reasons, records may be moved between systems and locations. Requirements for controls over such transfers are listed in section 4.4.

Requirements for controls concerning authenticity of records are listed in section 4.5.

Finally, requirements for security of protectively-marked documents (as typically are found in some government departments and their contractors) are listed in section 4.6.

4.1 Access

Organisations generally need to control access to their records. Typically, they need to limit or permit access to specific records and files by user and/or by group of users. Where matters of national security are involved, they may also take users' security clearances into account.

The setting of these access rights must be limited to certain roles. In the table in 13.4, this is shown as the Administrator role. Note however that this role is only implementing, from a system perspective, decisions taken by more senior management. Such decisions are typically based on laws and regulations, such as information laws, data security laws, archival laws and industry regulations; these are addressed in section 11.5.

Ref.	Requirement
4.1.1	The ERMS must allow the Administrator to limit access to records, files and metadata to specified users or user groups.
4.1.2	The ERMS must allow the Administrator to attach to the user profile attributes which determine the features, metadata fields, records or files to which the user has access. The attributes of the profile will: • prohibit access to the ERMS without an accepted authentication mechanism attributed to the user profile; • restrict user access to specific files or records; • restrict user access to specific classes of the classification scheme; • restrict user access according to the user's security clearance; • restrict users access to particular features (e.g. read, up-date and/or delete specific metadata fields); • deny access after a specified date; • allocate the user to a group or groups. *An example of an accepted authentication mechanism is a password.*
4.1.3	The ERMS must be able to provide the same control functions for roles as for users. *This feature allows the Administrators to manage and maintain a limited set of role access rights rather than a larger number of individual users. Examples of roles might include Manager, Claims Processing Clerk, Security Analyst, Database Administrator.*
4.1.4	The ERMS must be able to set up groups of users that are associated with a set of files or records. *Examples of groups might be Personnel, Sales team.*
4.1.5	The ERMS must allow a user to be a member of more than one group.
4.1.6	The ERMS must allow only Administrators to set up user profiles and allocate users to groups. *See also section 13.4.*
4.1.7	The ERMS should allow a user to stipulate which other users or groups can access records that the user is responsible for. This function should be granted to the user by the Administrator according to the organisation's policy.
4.1.8	The ERMS must allow changes to security attributes for groups or users (such as access rights, security level, privileges, password allocation and management) to be made only by Administrators.

Ref.	Requirement
4.1.9	If a user requests access to, or searches for, a record, volume or file which he does not have the right to access, the ERMS must provide one of the following responses (selectable at configuration time): • display title and metadata; • display the existence of a file or record (i.e. display its file or record number) but not its title or other metadata; • do not display any record information or indicate its existence in any way. *These options are presented in order of increasing security. Note that the requirement in the third option (i.e. the most stringent) implies that the ERMS must not include such records in any count of search results; this level of security is normally appropriate for records dealing with matters such as national security.*
4.1.10	If a user performs a full text search, the ERMS must never include in the search result list any record which the user does not have the right to access. *Note that if the first option of requirement 4.1.9 is chosen, this could be seen to conflict. This apparent conflict is intentional, for if this requirement is not present users may be able to use text searches to investigate the contents of documents to which they are not allowed access. Consequently this requirement must take precedence over requirement 4.1.9.*
4.1.11	If the ERMS allows users to make unauthorised attempts to access files, volumes or records, it must log these in the audit trail. *It will be acceptable for this feature to be controllable so that it only applies to administrator-specified security categories (as defined in 4.6).*
4.1.12	If the ERMS maintains a file repertory (see 3.2.10), it must be able to limit users' access to parts of the repertory which are specified at configuration time.

4.2 Audit trails

An audit trail is a record of actions taken which involve the ERMS. This includes actions taken by users or Administrators, or actions initiated automatically by the ERMS as a result of system parameters. See the Glossary at section 13.1 for a formal definition. The audit trail for records can be viewed as metadata of the records (because it consists of information describing some aspects of the records' history), though this is not essential.

The ERMS must be capable of management and control of electronic records according to the standards necessary for compliance with requirements for legal admissibility and security, and must be capable of demonstrating this compliance. The audit trail is a key factor in meeting these requirements by maintaining a complete record of all the actions on every record.

The volume of audit trail information can become large if all actions are audited. Consequently, in some implementations, management may decide that the selected actions need not be audited; and in most cases, the on-line audit trail is periodically moved to off-line storage, and is subject to deletion if and when the relevant records are disposed of. These are matters of management policy and/or legal/regulatory requirements; thus this specification includes system requirements to allow these actions, but does not establish the extent to which they are used.

Ref.	Requirement
4.2.1	The ERMS must keep an unalterable audit trail capable of automatically capturing and storing information about: • all the actions that are taken upon an electronic record, electronic file or classification scheme; • the user initiating and or carrying out the action; • the date and time of the event. *The word "unalterable" is to mean that the audit trail data cannot be modified in any way or deleted by any user; it may be subject to re-organisation and copying to removable media if required by, for example, database software, so long as its contents remains unchanged.*
4.2.2	Once the audit trail functionality has been activated, the ERMS must track events without manual intervention, and store in the audit trail information about them.
4.2.3	The ERMS must maintain the audit trail for as long as required, which will be at least for the life of the electronic records or electronic files to which it refers.
4.2.4	The ERMS must provide an audit trail of all changes made to: • groups of electronic files; • individual electronic files; • electronic volumes; • electronic records; • electronic documents; • metadata associated with any of the above.
4.2.5	The ERMS must provide an audit trail of all changes made to administrative parameters. *For example, if the Administrator changes a user's access rights.*

Ref.	Requirement
4.2.6	The ERMS must be capable of capturing and storing in the audit trail information about the following actions: • the date and time of capture of all electronic records; • re-classification of an electronic record in another electronic volume (see 3.4.2); • re-classification of an electronic file within the classification scheme (see 3.4.1); • any change to the retention schedule of an electronic file; • any change made to any metadata associated with classes, electronic files or electronic records; • date and time of creation, amendment and deletion of metadata; • changes made to the access privileges affecting an electronic file, electronic record or user; • export or transfer actions carried out on an electronic file; • date and time of a rendition (see the Glossary at section 13.1); • deletion / destruction actions on an electronic file or electronic record.
4.2.7	The ERMS should allow the audit trail facility to be configurable by the Administrator so that he can select the functions for which information is automatically stored; and the ERMS must ensure that this selection and all changes to it are stored in the audit trail.
4.2.8	The ERMS must ensure that audit trail data is available for inspection on request, so that a specific event can be identified and all related data made accessible, and that this can be achieved by authorised external personnel who have little or no familiarity with the system.
4.2.9	The ERMS must be able to export audit trails for specified electronic records, electronic files and groups of files (without affecting the audit trail stored by the ERMS). *This functionality can be used by external auditors who wish to examine or analyse system activity.*
4.2.10	The ERMS must be able to capture and store violations (i.e. a user's attempts to access a record, volume or file to which he is denied access), and (where violations can validly be attempted) attempted violations, of access control mechanisms. *For an illustration of circumstances which can allow attempts at violation, see 4.1.9.*

Ref.	Requirement
4.2.11	The ERMS must at a minimum be able to provide reports for actions on classes, files and records organised: • by record or file or class; • by user; • in chronological sequence.
4.2.12	The ERMS should be able to provide reports for actions on files and records organised by workstation and (where technically appropriate) by network address.

4.3 Backup and Recovery

Both business and regulatory demands require that an ERMS be provided with comprehensive controls to provide regular backup of the records and metadata; and to be able to recover rapidly records if any are lost because of system failure, accident, security breach etc.

Regular automated backup and recovery can be provided by the ERMS, or by integration with the services or utilities of an Electronic Document Management system (EDMS), or by a Database Management System operating with the ERMS.

In practice, backup and recovery functions may be divided between ERMS Administrators and staff in the organisation's IT operations area.

Ref.	Requirement
4.3.1	The ERMS must provide automated backup and recovery procedures that allow for regular backup of all or selected classes, files, records, metadata and administrative attributes of the ERMS repository.
4.3.2	The ERMS must allow the Administrator to schedule backup routines by: • specifying the frequency of backup; • selecting classes, files or records to be backed up; • allocating storage media, system or location for the backup (e.g. off line storage, separate system, remote site).
4.3.3	The ERMS must allow only the Administrator to restore from ERMS backups. Full integrity of the data must be maintained after the restore.
4.3.4	The ERMS must allow only the Administrator to roll-forward the ERMS from a backup to a more recent state, maintaining full integrity of the data.
4.3.5	The ERMS should be able to notify users whose updates may have been incompletely recovered, when they next use the system, that a potentially incomplete recovery has been executed.

Ref.	Requirement
4.3.6	The ERMS must allow users to indicate that selected records are considered to be "vital records". *Vital records are those records that are absolutely necessary to the organisation's ability to continue its business either in terms of its ability to cope with emergency/disaster conditions or to protect its financial and legal interests. The identification and protection of such records, therefore, is of great importance to any organisation.*
4.3.7	The ERMS should allow vital records and other records to be restored in distinct operations.

4.4 Tracking Record Movements

During their life cycle, files and their metadata may be transferred from one storage medium or location to another, as their activity decreases and/or their use changes. This transfer can be locally to either near-line (e.g. to removable media in an automated device, such as CD-Rs in a jukebox), offline (e.g. to a local or remote storage area) or to another record repository (e.g. a state or national archive). A tracking feature is needed to record the change of location for both ease of access and to meet regulatory requirements.

Ref.	Requirement
4.4.1	The ERMS must provide a tracking feature to monitor and record information about the location and movement of files, both electronic and physical.
4.4.2	The tracking function must record information about movements which includes: • unique identifier of the file or records; • current location as well as a user-defined number of previous locations (locations should be user-defined); • date file sent/moved from location; • date file received at location (for transfers); • user responsible for the move (where appropriate).
4.4.3	The ERMS must maintain access to the electronic record content, including the ability to render it, and including maintenance of its structure and formatting, over time and through generations of office application software. *This may be, but does not have to be, by use of a multi-format viewer application. Section 11.7 provides further details on long-term rendition issues.*

4.5 Authenticity

Corporate policy and the record-keeping requirements of business processes will determine which records should be captured, and when. It is essential that once the record is captured, all record components, structure and metadata necessary to ascertain the record is authentic shall not be changed. The captured records must be sustained in a non-revisable form and protected against intentional or accidental changes to their content, context, structure and appearance throughout their life to retain their authenticity.

Ref.	Requirement
4.5.1	The ERMS must restrict access to system functions according to user's role and strict system administration controls. *This is needed to protect the authenticity of electronic records*
4.5.2	Where possible and appropriate, the ERMS should be able to provide a warning if an attempt is made to capture a record which is incomplete or inconsistent in a way which will compromise its future apparent authenticity. *For example, a purchase order without a valid electronic signature, or an invoice from an unrecognised supplier.*
4.5.3	Where possible and appropriate, the ERMS should be able to provide a warning if an attempt is made to capture a record when the future verification of its authenticity is not possible.
4.5.4	The ERMS must prevent any change to the content of the electronic record by users and Administrators (except where change is part of the business and/or documentary process, as discussed elsewhere in this specification).

4.6 Security Categories

Section 4.1 describes requirements for controlling access by user and group. In some environments, notably those involving national security, there is a need to limit access further, using a scheme of security categories and security clearances. These clearances take precedence over any access rights which might be granted using features defined in section 4.1. The requirements in this section apply only in environments which have this need.

This is achieved by allocating to classes, files and/or records one or more "Security Categories". The term "Security Category" is used in this specification to mean "One or several terms associated with a record which define rules governing access to it." Note that this term is used expressly for this specification; it is not generally employed.

Users can then be allocated one or more security clearances which prevent access to all classes/files/records at higher security categories.

Security categories can be made up of sub-categories. Some sub-categories are hierarchic in nature. Other sub-categories may be arranged differently, typically in a way which is unique to an organisation or sector. This specification describes in detail only the requirements for a hierarchic sub-category.

Ref.	Requirement
4.6.1	The ERMS must allow security categories to be assigned to records.
4.6.2	The ERMS must allow one of the following to be selected at configuration time: • security categories to be assigned to classes, files and/or volumes; • electronic classes, files and/or volumes not to bear security categories. *This is desirable because while some organisations prefer to assign security categories to electronic files, mimicking the functionality of paper records and physical files, others prefer to protect only the underlying records.*
4.6.3	The ERMS security subsystem should be capable of being employed effectively together with general security products.
4.6.4	The ERMS must allow, but not necessarily require, security categories to be made up of one or more "sub-categories". *For example, a security category may be made up of three sub-categories, as in the following fictitious example:*

Sub-category	***Allowable values***
Class	*Top Secret* *Secret* *Confidential* *Restricted* *Unclassified*
Caveat	*NATO Eyes Only* *WEU Eyes Only*
Descriptor	*Commercial* *Personnel* *Management* *Audit and Accounts*

In this fictitious example, the sub-category "Class" is hierarchic (see 4.6.6) while the other sub-categories are not. Requirements for hierarchic sub-categories are common; these are specified below. However, requirements for hierarchic sub-categories can be complex; with the exception of requirement 4.6.5 they are not detailed here.

Ref.	Requirement
4.6.5	The ERMS should allow specific implementations of complex or unique security rules. *This may be provided by suitable application program interfaces. It is necessary where there is a need to manage records using marking conventions not covered here such as IDO (International Defence Organisation) markings or access restrictions for medical records.*
4.6.6	For at least one sub-category, the ERMS must support a hierarchy of at least five levels, from unrestricted access at the lowest level to highly restricted access at the highest level. *The sub-category "class" in requirement 4.6.4 is an example of this.*
4.6.7	The ERMS must allow security clearances to be assigned to users, these clearances to match the sub-category. *To continue the example in 4.6.4, users would be assigned one of the following clearances:* *Top Secret* *Secret* *Confidential* *Restricted* *Unclassified*
4.6.8	The ERMS must deny users access to electronic records (and classes and electronic files depending on the selection made for 4.6.2) which have a security category higher than their security clearance. *Note that the correct level of security clearance may not be sufficient to obtain access. Access to the electronic records may in addition be restricted to specified users, roles and/or groups, using features described in section 4.1.*
4.6.9	The ERMS must support the automated application of a default value of the lowest level of security in the sub-category to a class, electronic file or record not allocated any other security category. *For example, continuing the example in 4.6.4, the default would be "Unclassified".*
4.6.10	The ERMS should be capable of preventing an electronic file from having a lower security classification category than any electronic record within that file (depending on the selection made for 4.6.2).
4.6.11	The Administrator should be able to determine the highest security category of any record in any class or file by means of one simple enquiry. *In some environments, this will be an important feature to aid manageability.*
4.6.12	The ERMS should support routine, scheduled, review of security categories.

5 RETENTION AND DISPOSAL

A fundamental aspect of records management is the use of retention schedules to govern the removal of records from operational systems. Retention schedules define how long the records have to be kept by the ERMS, and how they may be disposed of. Requirements for retention schedules are listed in section 5.1.

The processes which can take place at the date specified by retention schedules are described in subsequent sections. Requirements for review processes are listed in section 5.2, and requirements for transfer, export and destruction are listed in section 5.3.

Terminology

As explained in section 2.2 under the heading Electronic File and Volume, records are sometimes managed in files and sometimes in file volumes. This applies at all stages of the processes described in this chapter. Therefore, for simplicity, the word "file" is used in this chapter to indicate "file or volume as appropriate".

5.1 Retention Schedules

Ref.	Requirement
5.1.1	The ERMS must provide a function that specifies retention schedules, automates reporting and destruction actions, and provides integrated facilities for exporting records and metadata.
5.1.2	The ERMS must be able to restrict the setting up and changing of retention schedules to the Administrator.
5.1.3	The ERMS must allow the Administrator to define and store a standard set of customised standard retention schedules.
5.1.4	The ERMS must be capable of associating a retention schedule with any record, file or class of a classification scheme. *The retention schedule can be selected from the standard set or entered manually when the file is opened.*

Ref.	Requirement
5.1.5	The ERMS should be capable of associating more than one retention schedule with any file or class of a classification scheme. *As examples,* • *a file may have one schedule which is the standard schedule for the organisation it belongs to, and a second schedule which is a special schedule related to litigation relying on this file;* • *a class may have a retention schedule governed by legislation, but a class within it may have a second retention schedule with different rules which arise from medical records retention regulations.*
5.1.6	Every record in a file or class must, by default, be governed by the retention schedule(s) associated with that file or class.
5.1.7	Each retention schedule must include a disposition decision (5.1.10), retention period (5.1.11), reason, and source for the decision.
5.1.8	For each file, the ERMS must • automatically track retention periods that have been allocated to the file or to the class in which it belongs; • initiate the disposal process once the end of the retention period is reached.
5.1.9	If more than one retention schedule is associated with a file or class, the ERMS must automatically track all retention periods specified in these retention schedules, and initiate the disposal process once the last of all these retention dates is reached.
5.1.10	The ERMS must allow at least the following decisions for each retention schedule: • retain indefinitely; • present for review at a future date, the date to be defined as in 5.1.11; • destroy at a future date, the date to be defined as in 5.1.11; • transfer at a future date, the date to be defined as in 5.1.11.

Ref.	Requirement
5.1.11	Each retention schedule must allow the retention periods (as defined in 5.1.10) to be specified for a future date, with the date being specified in at least the following ways: • passage of a specified period of time after the file is opened; • passage of a specified period of time after the file is closed; • passage of a specified period of time since the most recent record has been assigned to the file; • passage of a specified period of time since a record has been retrieved from the file; • passage of a specified period of time after a specific event (which event is described in the schedule, and will be notified to the ERMS by the Administrator rather than being detected automatically by the ERMS) (for example, "…after contract signature"); • specified as "indefinite" to indicate long term preservation of the records. *While the above is generally inclusive, it is possible that some kinds or records will have types of retention requirements which are not listed here.*
5.1.12	The ERMS must support retention periods of time from one month to one hundred years for requirement 5.1.11. *These minimum and maximum periods are suggested as arbitrary periods intended to avoid any practical limitation. While it is improbable that any ERMS will exist for one hundred years, a requirement of this nature will allow records to be exported to future systems without the need to revise retention schedules.*
5.1.13	The ERMS must automatically record and report all disposition actions to the Administrator.
5.1.14	The ERMS must enable a retention schedule to be assigned to a file that can take precedence over the retention schedule assigned to a class in which the file is assigned.
5.1.15	The ERMS must allow the Administrator to amend any retention schedule allocated to any file at any point in the life of the file.
5.1.16	The ERMS must allow the Administrator to change which schedule(s) is/are associated with a file at any point in the life of the file.
5.1.17	The ERMS should allow the definition of sets of processing rules which can be applied as an alerting facility to specified files and classes, prior to initiation of a disposal process. For example: • review of the file and contents by a specific manager or Administrator; • notify the Administrator when a file has a given security level.

Ref.	Requirement
5.1.18	When an Administrator moves electronic files or records between classes of the classification scheme, the ERMS should optionally allow the retention schedule of the destination class to replace the existing retention schedules(s) applying to these records.

5.2 Review

Review is the process of checking files, once they have reached the date or event specified by a retention schedule, to decide whether they are to be retained, transferred to another system, or destroyed. The reviewer may consider metadata, contents, or both. In some environments, the retention schedules are used to govern disposition without a review.

The disposition of certain records is subject to laws and regulations. Reviews must be performed in a way which is consistent with these laws and regulations, and where relevant in co-operation with responsible archival authorities. Further discussion of these issues is beyond the scope of this specification.

Ref.	Requirement
5.2.1	The ERMS should be able to notify the Administrator regularly of all retention schedules which will come into force in a specified period of time, and provide quantitative reports on the volumes and types of records.
5.2.2	The Administrator should be able to specify the frequency of a retention schedule report, the information reported and highlighting exceptions such as disposal overdue.
5.2.3	The ERMS must support the review process by presenting electronic files to be reviewed, with their metadata and retention schedule information (the reason), in a manner which allows the reviewer to browse (i.e. navigate and study) the file contents and/or metadata efficiently. *In practice, this implies features for navigating forward, back etc. within and between files, and from/to the metadata for files and records.*
5.2.4	The ERMS should alert the Administrator if an electronic file that is due for destruction is referred to in a link from another file; and must pause the destruction process to allow the following remedial action to be taken: • confirmation by the Administrator to proceed with or cancel the process; • generation of a report detailing the files or record(s) concerned and all references or links for which it is a destination.

Ref.	Requirement
5.2.5	The ERMS must allow the reviewer to take at least any of the following actions for each file during review: • mark the file for deletion; • mark the file for transfer (see 5.3.7); • change the retention schedule (or assign a different schedule) so that the file is retained and re-reviewed at a later date, the date to be defined as in 5.1.11.
5.2.6	The ERMS must allow the reviewer to enter comments into the file's metadata to record the reasons for the review decisions.
5.2.7	The ERMS must alert the Administrator to files due for disposal before implementing disposal actions; and on confirmation from the Administrator the ERMS must be capable of initiating the disposal actions specified in 5.1.10.
5.2.8	The ERMS should support reporting and analysis tools for the management of retention and retention schedules by the Administrator, including the ability to: • list all retention schedules; • list all electronic files to which a specified retention schedule is assigned; • list the retention schedule(s) applied to all files below a specified point in the hierarchy of the classification scheme; • identify, compare and review retention schedules (including their contents) across the classification scheme; • identify formal contradictions in retention schedules across the classification scheme.
5.2.9	The ERMS must store in the audit trail all decisions taken by the reviewer during reviews.
5.2.10	The ERMS should provide, or support the ability to interface with, a workflow facility to support the scheduling, review and export/transfer process, by tracking: • progress/status of the review, such as awaiting or in-progress, details of reviewer and date; • records awaiting disposal as a result of a review decision; • progress of the transfer process.
5.2.11	The ERMS should be able to accumulate statistics of review decisions in a given period and provide tabular and graphical reports on the activity.

5.3 Transfer, Export and Destruction

Organisations may need to move records from their ERMS to other locations or systems. This is referred to here as "transfer". Note that the term transfer is used even though only a copy is sent to the other location or system. Reasons for transfer may include:

- permanent preservation of the documents for legal, administrative or research reasons;
- to use outside services for the medium term or long term management of the records.

This action often results in the records being transferred to a different ERMS environment. Note that in some cases the records originally residing in the ERMS will be deleted from it after transfer, while in other cases they will be retained.

In other circumstances, the organisation will need to export the records, that is move a copy to another location or system while retaining the records. In yet other circumstances it will need to destroy the records.

In any event, the requirement is to execute the transfer, export or destruction in a controlled manner. In all cases, the metadata and audit trails must be considered at the same time as the records they relate to.

Note that in this context "destruction" is different from "deletion". Deletion of records under other circumstances is covered in section 9.3.

Ref.	Requirement
5.3.1	The ERMS must provide a well managed process to transfer records to another system or to a third party organisation.
5.3.2	Whenever the ERMS transfers any class, file or volume, the transfer must include: • (for classes) all files in the class; • (for files) all volumes below the file in the hierarchy; • all records in all these files and volumes; • all metadata associated with these files, records and volumes.

Ref.	Requirement
5.3.3	The ERMS must be able to transfer or export a file or class in one sequence of operations, such that: • the content and structure of its electronic records are not degraded; • all components of an electronic record, (when the record consists of more than one component) are exported as an integral unit; for example, an e-mail message with associated file attachments; • all links between the record and its metadata are retained; • all links between electronic records, volumes and files are retained.
5.3.4	Whenever the ERMS transfers or exports records, the ERMS must be able to include a copy of all the audit trail data associated with the records, volumes and files being transferred.
5.3.5	The ERMS should provide a utility or conversion tool to support the rendition of records marked for transfer or export into some approved transfer format(s). *For example, portable document format (PDF) or equivalent, and extensible mark-up language (XML).*
5.3.6	The ERMS must produce a report detailing any failure during a transfer, export or deletion. The report must identify any records destined for transfer which have generated processing errors, and any files or records which are not successfully transferred, exported or deleted.
5.3.7	The ERMS must retain all electronic files that have been transferred, at least until confirmation of a successful transfer process. *This is suggested as a procedural safeguard, to ensure that records are not deleted before successful transfer-in is reported from the recipient.*
5.3.8	The ERMS should be able to export an entire class of the classification scheme in one sequence of operations, ensuring that: • the relative location of each file in the classification scheme is maintained, so that the file structure can be reconstructed; • all metadata at higher points in the hierarchy is retained and moved with the class.
5.3.9	Where hybrid files are to be transferred, exported or destroyed, the ERMS should require the Administrator to confirm that the paper part of the same files has been transferred, exported or destroyed before transferring, exporting or destroying the electronic part.
5.3.10	The ERMS should provide the ability to add user-defined metadata elements required for archival management purposes to electronic files selected for transfer.
5.3.11	The ERMS should provide the ability to sort electronic files selected for transfer into ordered lists according to user-selected metadata elements.

Ref.	Requirement
5.3.12	The ERMS should provide the ability to generate user-defined forms to describe electronic files that are being exported or transferred.
5.3.13	The ERMS should enable the total destruction of classes and individual files that are stored on re-writable media, by completely obliterating them so that they cannot be restored by use of specialist data recovery facilities. *In some environments, this may require repeated over-writing of the data according to specified standards.* *Where an assurance of destruction is required, it may be necessary to consider the existence of copies on backup media. This is a procedural matter which is beyond the scope of this specification.*
5.3.14	If records are stored on write-once media, the ERMS must provide facilities to prevent access to them so that they cannot be restored by normal use of the ERMS or by standard operating system utilities. *This normally implies destruction of the index data (held on re-writable media), which stores the locations of the data on write-once media.* *Where an assurance of destruction is required, it may be necessary to consider the existence of copies on backup media. This is a procedural matter which is beyond the scope of this specification.*
5.3.15	The ERMS must have the ability to retain metadata for files and records which have been destroyed or transferred. *In some environments it is desirable to retain detailed information about records which have been destroyed. It can also allow simple identification of records which have been destroyed or transferred; it is closely related to 5.3.16.*
5.3.16	The ERMS must allow the Administrator to specify a subset of file metadata which will be retained for files which are destroyed, transferred out or moved offline. *This is desirable so that the organisation can still know what records it has held and the dates they were destroyed or disposed of, without necessarily incurring the overhead of keeping all the detailed metadata for the file.*
5.3.17	The ERMS must allow records to be transferred or exported more than once.

6 CAPTURING RECORDS

Terminology

The term "capture" is used to encompass the processes of registering a record, deciding which class it is to be classified to, adding further metadata to it, and storing it in the ERMS.

In the context of an ERMS, the registration and other processes may be separate or indistinguishable.

Formal definitions are given in the Glossary in section 13.1.

Overview

This chapter covers requirements relating to getting records into an ERMS. The first section (6.1) covers the standard capture process. The following section (6.2) covers the bulk import of records from other systems. Section (6.3) describes considerations for particular kinds of document; and, because of the increasing importance of e-mail, this is followed by a section devoted to e-mail (6.4).

6.1 Capture

This section contains requirements for the capture process.

Electronic documents that are generated or received in the course of business processes originate from both internal and external sources. The electronic documents may be in various formats, may be produced by different authors; and may be received as single documents and as multiple document files. They may arrive through different communication channels e.g. local area network, wide area network, electronic mail, facsimile, letter post (to be scanned) and at variable arrival rates and volumes. A flexible input system is required to capture documents with good management controls so that these diverse requirements are addressed.

Ref.	Requirement
6.1.1	The ERMS record capture process must provide the controls and functionality to: • register and manage all electronic records regardless of the method of encoding or other technological characteristics; • ensure that the records are associated with a classification scheme and associated with one or more files; • integrate with application software that generates the records; • validate and control the entry of metadata into the ERMS.
6.1.2	The ERMS must be able to take into the electronic record management environment: • the content of the electronic record, including information defining its form and rendition and information defining the structure and behaviour of the electronic record, retaining its structural integrity (for example, all the components of an e-mail message with attachment(s), or of a web page, with their links); • information about the electronic document, for example, the file name; • the date of creation and other document metadata about the elements of the record; • information about the context in which the electronic record was originated, created and declared, for example its business process and, originator(s), author(s); • information about the application program which generated the record, including its version. *Information about rendition is sometimes implicit in the computer file name extension, e.g. ".doc" or ".pdf". This will be acceptable in many cases, though it may not suffice in cases where long-term preservation is needed, or where precision is needed (for example, precision of colour space).*
6.1.3	The ERMS must allow the capture acquisition of all metadata elements specified at systems configuration, and retain them with the electronic record in a tightly-bound relationship at all times.
6.1.4	The ERMS must ensure that the content of selected elements of the metadata of the electronic record can only be changed by authorised users and Administrators.

Ref.	Requirement
6.1.5	The ERMS should support the ability to assign the same electronic records to different electronic files, from one electronic document without physical duplication of the electronic record. *For example an invoice might be added to a supplier file by one user, and to a product file by another. In another example, one user may choose to add a document which concerns two subjects to the two relevant files.* *This is normally achieved by the use of pointers.*
6.1.6	The ERMS must support automated assistance in registration of electronic documents, by automatically extracting metadata, for at least the following types of document: • office documents (e.g. word-processed letters in a standard format); • e-mail without attachments, both incoming and outgoing; • e-mail with attachments, both incoming and outgoing; • facsimile messages, both incoming and outgoing.
6.1.7	The ERMS must record the date and time of registration as metadata. *If the date and time are part of the unique identifier, and as long as they can be explicitly extracted from this number, it is not necessary to store the date and time separately.* *The accuracy of the time will depend on the application.*
6.1.8	The ERMS must ensure that every registered record has a viewable registry entry including the following metadata specified at configuration time. *Some of the required metadata may already be present, or may be extracted automatically from the record. The ERMS must require remaining metadata to be entered.*
6.1.9	The ERMS must allow entry of further descriptive and other metadata at: • time of registration; and/or: • a later stage of processing.
6.1.10	Where a document has more than one version, the ERMS must allow users to choose at least one of the following: • register all versions of the document as one record; • register one version of the document as a record; • register each version of the document as a record.

Ref.	Requirement
6.1.11	The ERMS should provide automated support for decisions on the classification of electronic records to electronic files by means of some or all of the following: • making only a subset of a classification scheme accessible to a user or role; • storing for each user or role a list of that user's most recently used files; • suggesting the most recently used files by that user; • suggesting files which contain related electronic records; • suggesting files by inferences drawn from record metadata elements: for example, significant words used in the document title; • suggesting files by inferences drawn from the record contents.
6.1.12	The ERMS should allow a user to pass electronic records to another user to complete the process of capture.
6.1.13	For electronic records that are constructed of more than one component, the ERMS must: • handle the record as a single indivisible record, retaining the relationship between the components; • retain the record's structural integrity; • support later integrated retrieval, display, management; • manage disposal of all components of the electronic record as a whole unit (i.e. in one operation). *Examples of such records are web pages with embedded graphics.*
6.1.14	The ERMS must support automated assistance in registration of electronic documents, by automatically extracting as much metadata as possible, for as many kinds of document as possible. *The rationales for this requirement are to minimise the amount of data entry performed by users and to increase the accuracy of metadata. The metadata elements involved, and the kinds of document for which this is possible, will depend on the environment. As an example, in an office situation dealing with unstructured and semi-structured text documents it would be reasonable to include:* • *word-processed letters, memoranda and other documents prepared using templates, standard to the organisation, which allow automated identification of metadata elements;* • *e-mail with or without attachments, both incoming and outgoing;* • *outgoing facsimile messages.*
6.1.15	The ERMS must issue a warning if a user attempts to register a document which has already been registered in the same file.

6.2 Bulk importing

Records may reach the ERMS in bulk in a number of ways. For example, from another ERMS, as an electronic file made up of a number of records of the same type (e.g. daily invoices) or a bulk transfer from an EDMS. The ERMS must be able to accept these, and must include features to manage the capture process.

Ref.	Requirement
6.2.1	The ERMS must provide the ability to capture transactional documents generated by other systems. This must include: • supporting predefined batch file transaction imports; • providing edit rules to customise the automatic registration of the records; • maintaining data integrity validation.
6.2.2	The ERMS system must provide facilities to manage input queues.
6.2.3	The ERMS should be able to set up multiple input queues for different document types. *For example, in different environments, queues might be for e-mails, scanned correspondence, documents from a department, group or individual, transactions from a computer applications, or documents from a document management system.*

6.3 Types of Document

Overview

Organisations will need to capture a diverse range of types of documents with different formats and structures. The technical requirements for capture will vary according to the complexity of the documents. In some environments, it is not possible to identify all the kinds of documents in advance, as some are received from external sources.

Self-modifying documents

There is sometimes a requirement to capture documents which appear to be, or which are, self-modifying. This can give rise to complex requirements which are examined here in outline rather than in detail.

Some documents appear to be self-modifying, that is they seem to change their contents without user intervention. A common example is word processing or spreadsheet documents which contain a “field” or “code” which automatically displays the current date. The rendition (see the Glossary at section 13.1) of the document varies according to the date on which it is rendered. In extreme cases, the “field” or “code” can vary so much as to change the appearance of a document radically (for example a code which displays the documents full directory path: in

some cases, changes in the path, caused by a long path name in a large hierarchic ERMS, can cause major changes in pagination). However, the document is not truly modified; only its rendition changes, and this according to the software used to view it. While documents which appear self-modifying do not contravene the requirement that record contents must be fixed, they can appear to do so. For this reason, they are best avoided.

In other cases, documents may contain code which truly modifies the document, such as a spreadsheet with a sophisticated "macro" which changes the spreadsheet (by means of the application software used to view it) and then automatically saves it. In these cases, there is a risk that the document will change itself during the capture process, depending on details of the process and the ERMS controls. This is clearly unacceptable.

In most cases, documents which are self-modifying in this way should be avoided, stored in a format which disables the self-modifying code, or else viewed only with software which does not trigger the modification. If the self-modifying code is itself an essential part of the record, appropriate steps should be decided based on the specifics of the case.

For documents which can be printed, examples of formats which disable self-modifying code may be the Adobe's proprietary PDF, or Tumbleweed Software's proprietary ENVOY. In this case, it is important to ensure that the conversion to the desired format is performed in a way which does not cause the documents to modify themselves in an undesirable way; for example, in the case of a self-modifying date in a letter, the conversion should take place on the date which is shown in the letter.

Where storage of documents which are self-modifying, or which appear to be so, is unavoidable information about these characteristics should be stored with the records in their metadata.

Ref.	**Requirement**
6.3.1	The ERMS must be able to capture documents from a range of different electronic document format types and structures as records. *This range should be specified before a system is evaluated using this specification.*

Ref.	Requirement
6.3.2	The ERMS must support the capture of the most commonly used office documents. These include both simple and complex documents types. Types of document formats supported must include: • Simple: facsimile, office documents, presentations, text, image, e-mail messages (see section 6.4), voice; • Compound: electronic mail with attachments, desktop publishing, web pages, graphics. *The list of document types that the ERMS must support will vary from organisation to organisation.*
6.3.3	The document formats supported for 6.3.2 must be extendable as new formats are introduced.
6.3.4	The ERMS should be able to capture the following types of documents: • electronic calendars; • information from other computer applications e.g., Accounting, Payroll, Computer Aided Design; • scanned paper documents; • voice files; • video clips; • digital schematics and maps; • structured data (e.g. EDI transactions); • databases; • multimedia documents. *The list of document types that the ERMS should support will vary from organisation to organisation.*
6.3.5	The ERMS must not impose any practical limit on the number of records which can be captured in a file, or on the number of records which can be stored in the ERMS.
6.3.6	The ERMS should allow a compound document to be captured in either of two ways: • as a single compound record; • as a series of linked simple records, one per component of the compound document.

6.4 E-mail Management

Electronic mail is used for sending both simple messages and documents (attachments), within and between organisations. The characteristics of electronic mail can make it difficult to track and register. Organisations require to be able to enforce management controls to:

- capture all inbound and outbound electronic mail messages and attachments;

and/or to:

- provide users with the capability of capturing selected e-mail messages and attachments.

The latter option requires the users to assess the relevance and importance of items, and the risks of not capturing them.

Ref.	Requirement
6.4.1	The ERMS must allow one of the following modes of operation to be chosen at configuration time: • the ERMS allows users to capture e-mails (i.e. after choosing which if any to register); or • the ERMS provides an automated process for the capturing of all inbound and outbound e-mails.
6.4.2	The ERMS should allow individual users to process and capture their incoming e-mail messages from within their e-mail system. The user should be able to process each e-mail in the inbox, from within their e-mail system, as follows: • view each mail message and an indication of its attachments (if any); • view the contents of the attachments using multi-format document viewer; • register the mail message and its attachments as a new record in ERMS; • link the mail message and its attachments to an existing record in ERMS.
6.4.3	The ERMS should ensure the capture of a human-readable version of an e-mail message address, where one is associated with the original message; for example, ‘Jan Schmidt’ rather than ‘jsa97@xyz.int’.

7 REFERENCING

The various entities of the ERMS (classes, files, volumes, records) need identifiers. These identifiers must be unique for each occurrence of each entity; the uniqueness must extend either across the entire ERMS or within the relevant hierarchic level. As the requirements for these references are common, they are brought together here for classes, files, volumes, and records.

Ref.	Requirement
7.1.1	Whenever a new occurrence of any of the following is created in the ERMS, the ERMS must associate with it a unique identifier (as defined below): • class; • file; • volume; • record; • record extract.
7.1.2	All unique identifiers in the ERMS must be either: • unique within the entire ERMS; or: • unique within the next higher level of the appropriate branch of the hierarchy within which it appears). *As an example of the second option, the path* *Contracts : Company name : Correspondence* *is unique, but its final segment may be repeated in a different path, e.g.* *Regional plan development : Public consultation : Correspondence*
7.1.3	The ERMS must be able to store the unique identifiers as metadata elements of the entities to which they refer.
7.1.4	The ERMS should allow the format of the unique identifier to be specified at configuration time. *The identifier may be a number or alphanumeric, or may include the concatenated identifiers of the volume and electronic files above the record in the classification scheme.*

Ref.	Requirement
7.1.5	The ERMS must either: • generate the unique identifier automatically and prevent users from inputting the unique identifier manually, and from subsequently modifying it (for example, a sequential number); or: • allow users to input the unique identifier, but validate that it is unique before it is accepted (for example, an account number). *An option is to generate the unique identifier automatically, but then to conceal it from the user, allowing the user to enter a non-unique string (e.g. a surname) as an "identifier." The user would use this string as an identifier, but the ERMS would view it as searchable user-defined metadata.*
7.1.6	When creating a new electronic class or file in a classification scheme which uses a structured numerical coding reference based on sequential numbering, the ERMS should automatically generate the next sequential number available at that position within the classification scheme. *For example, if a class of the classification scheme already contains the files:* *900 - 23 - 01 Manufacturing : Order Processing : Sales Order Validation* *900 - 23 - 02 Manufacturing : Order Processing : Invoicing* *900 - 23 - 03 Manufacturing : Order Processing : Credit Note Processing* *Then if the Administrator adds a new file to this class, the ERMS should automatically assign it the reference 900 - 23 - 04.* *Likewise, if the Administrator adds a new class to the "Manufacturing" class the ERMS should automatically assign it the reference 900 - 24.*
7.1.7	When an ERMS automatically generates unique identifiers, it should allow the Administrator to specify at configuration time the starting number (e.g. 0, 00, 100) and increment (e.g. 1, 10) to be used in all cases.

8 SEARCHING, RETRIEVAL AND RENDERING

An integral part of an ERMS is the ability for the user to retrieve files and records. This includes searching for them when precise details are not known, and rendering them. Rendering is producing a representation on-screen ("displaying") or printing; it may also imply playing audio and/or video (see Glossary, section 13.1).

Accessing files and records, and then viewing records will require a flexible and broad range of searching, retrieval and rendering functions to meet the demands of the different types of user. Although this can be thought of as not being classically a records management function, the required functionality is described here on the grounds that an ERMS without good retrieval facilities is of limited value.

This chapter lists requirements for searching and retrieval in section 8.1. Requirements associated with rendering are divided into three sections: section 8.2 lists requirements for display, section 8.3 deals with printing, and section 8.4 addresses rendering of records which cannot be printed.

Security

All of the features and functionality in this chapter must be subject to access controls as described elsewhere in this specification, including security controls. In other words, the ERMS must never present information to any user which that user is not entitled to receive. To avoid complexity, this is assumed and is not repeated in each detailed requirement.

8.1 Search and Retrieval

Searching is the process of identification of records or files through user-defined parameters for the purpose of confirming, locating, accessing and retrieving records, files and/or their metadata.

The ERMS search and navigation tools to locate metadata, records, volumes or files requires a range of searching techniques for the sophisticated "research" user and support for the casual and less "computer literate" operator.

Ref.	Requirement
8.1.1	The ERMS must provide a flexible range of functions that operate on the metadata related to every level of record aggregation (file, class) and on the contents of the records through user-defined parameters for the purpose of locating, accessing and retrieving records and/or metadata either individually or in aggregation.

Ref.	Requirement
8.1.2	The ERMS search facilities should be integrated and should, to users, appear the same for all levels of the classification scheme. *In other words, users should see the same interface, features and options whether searching for classes, files or records.*
8.1.3	In the case of files, the ERMS should present seamless functionality across searches for electronic files, hybrid files (see 10.1) and physical files.
8.1.4	The ERMS must allow all record, volume and file metadata to be searchable.
8.1.5	The ERMS must allow the text contents of records to be searchable.
8.1.6	The ERMS must allow the user to set up a single search request with combinations of metadata and/or record content.
8.1.7	The ERMS must allow Administrators to configure and change the search fields including: • specify any element of record, volume and file metadata, and optionally full record content as search fields; • change the search field configuration.
8.1.8	The ERMS must provide searching tools that cover the following techniques: • free text searching of combinations of record and file metadata elements and record content; • Boolean searching of metadata elements.
8.1.9	The ERMS should provide the free text and metadata searching in an integrated and consistent manner.
8.1.10	The ERMS should provide concept searching by the use of a thesaurus incorporated as an on-line index. *This will allow retrieval of documents with a broader, narrower, or related term in their content or metadata. For example, a search for "ophthalmic services" might retrieve "health services", "eye test" or "ophthalmology".*
8.1.11	The ERMS must provide for "wild card" searching of metadata that allows for forward, backward and embedded expansion. *For example, the search term "proj*" might retrieve "project" or "PROJA"; the term C*n would retrieve" Commission".*
8.1.12	The ERMS should provide word proximity searching that can specify that a word has to appear within a given distance of another word in the record to qualify as a hit.

Ref.	Requirement
8.1.13	Where a graphical user interface is employed, the ERMS must provide a browsing mechanisms that provides graphical or other display browsing techniques at both the class and file level. *This would be used with the searching techniques described above to provide a first level view of metadata for a group of records or files which have met the specified search criteria.*
8.1.14	The ERMS must allow searching within an electronic file (at any level in the classification scheme hierarchy) or across files.
8.1.15	The ERMS must be able to search for and retrieve a complete electronic file, or file volume, and all its contents and contextual metadata, and render all, and only, those entries in the context of that file as a discrete group and in a single retrieval process. *This is needed, for example, when a user wishes to print a file in its entirety to take to a meeting, or to facilitate temporary working with paper for any other reason.*
8.1.16	The ERMS must be able to search for, retrieve and render an electronic file by all implemented naming principles, including: • file name; • file identifier (classification code).
8.1.17	The ERMS must display the total number of hits from a search on the user's screen and must allow the user to then display the search results (the "hit list"), or refine his search criteria and issue another request.
8.1.18	The ERMS must allow records, files etc. listed in a hit list to be selected then opened (subject to access controls) by a single click or keystroke.
8.1.19	The ERMS should allow the metadata of any object (such as record, volume, file or class) to be searched using the techniques in this section whether the object itself is in electronic form or not, and regardless of whether the object is stored on-line, near-line or off-line.
8.1.20	The ERMS should allow users to save and re-use queries.
8.1.21	The ERMS should allow users to refine (i.e. narrow) searches. *A user should for example be able to start with the hit list from a search, then launch a further search within that list.*
8.1.22	The ERMS should allow the use of named time intervals in search requests, e.g. "last week", "this month". *This is in contrast to the specification of intervals by calendar dates or numbers of days.*

Ref.	Requirement
8.1.23	The ERMS must allow users to retrieve files and records directly by a unique identifier. *If the unique identifier is not accessible to the user (see note to 7.1.5) this is not relevant.*
8.1.24	The ERMS should provide display formats configurable by users or Administrators for search results, including such features and functions as: • select the order in which the search results are presented; • specify the number of hits displayed on the screen per view from the search; • set the maximum number of hits for a search; • save the search results; • choose which metadata fields are displayed in search result lists.
8.1.25	The ERMS should provide relevance ranking of the search results.
8.1.26	The ERMS should be able to relate an "extract" of an electronic record (see section 9.3) to the original record, so that retrieval of one allows retrieval of the other, whilst retaining separate metadata and access controls over the two items.
8.1.27	When viewing or working with a record or aggregation (e.g. file or class) of records, whether as the result of a search or not, a user should be able to use ERMS features to find information about the next-higher level of aggregation of records easily and without leaving or closing the record. *For example, when reading a record, the user should be able to find out what volume and file it is in; if viewing file metadata, the user should be able to find out information about the class in which it is located.*
8.1.28	No ERMS search or retrieval function must ever reveal to a user any information (metadata or record content) which the access and security controls (sections 4.1 and 4.6 respectively) are intended to hide from that user.
8.1.29	The ERMS should include the ability to control access to records based on intellectual property restrictions, and generate charging data for such accesses. *This brief statement encompasses a wide range of functionality which is beyond the scope of this specification. This requirement may be satisfied by providing the ability to link to a separate application system.*

8.2 Rendering: Displaying Records

An ERMS may contain records with different formats and structures. The user requires generic viewing facilities that will accommodate displaying, rendering and printing a range of formats.

Ref.	Requirement
8.2.1	The ERMS must render records that the search request has retrieved. *If the ERMS is storing records in a proprietary application format, it may be acceptable for the rendering to be performed by an application outside the ERMS.*
8.2.2	The ERMS should render records that the search request has retrieved without loading the associated application software. *This is typically provided by integrating in the ERMS a viewer software package. This is frequently desirable to increase speed of rendering.*
8.2.3	The ERMS should be able to render all the types of electronic records specified by the organisation in a manner that preserves the information of the records (e.g. all the features of visual presentation and layout produced by the generating application package), and which renders all components of an electronic record together. *The organisation needs to specify the application packages and formats required.*

8.3 Rendering: Printing

This section applies to records which can meaningfully be printed, and control information within the ERMS.

The ERMS must provide printing facilities, to allow all users to obtain printed copies of records and their metadata, and of other information. In all cases, "printing" is understood to be at the application level, with all the controls and features usually provided (such as multi-page reports, headings, use of any suitable configured printer). Sending screen image dumps to a printer is not normally considered acceptable for this requirement.

Ref.	Requirement
8.3.1	The ERMS must provide the user with flexible ways of printing records and their relevant metadata, including the ability to print a record(s) with metadata specified by the user.
8.3.2	The ERMS must allow the printing of metadata for a file.
8.3.3	The ERMS must allow all the records in a file to be printed, in the sequence specified by the user, in one operation.
8.3.4	The ERMS must allow the user to be able to print out a summary list of selected records (e.g. the contents of a file), consisting of a user-specified subset of metadata elements (e.g. Title, Author, Creation date) for each record.

Ref.	Requirement
8.3.5	The ERMS should allow the Administrator to specify that all printouts or records have selected metadata elements appended to them, e.g. title, registration number, date, security category.
8.3.6	The ERMS must allow users to print search result hit lists.
8.3.7	The ERMS must allow the Administrator to print any and all administrative parameters.
8.3.8	The ERMS must allow Administrators to print retention schedules.
8.3.9	The ERMS should allow Administrators to print the thesaurus.
8.3.10	The ERMS must allow Administrators to print the classification scheme.
8.3.11	The ERMS must allow Administrators to print the file repertory (if used; see 3.2.10).
8.3.12	The ERMS must allow Administrators to print audit trails (see 4.2).
8.3.13	The ERMS must be able to print all the types of electronic records specified by the organisation. Printing must: • preserve the layout produced by the generating application package(s); • include all (printable) components of the electronic record. *The organisation needs to specify the application packages and formats required.*

8.4 Rendering: Other

This section applies only to records which cannot meaningfully be printed.

Ref.	Requirement
8.4.1	The ERMS must include features for outputting to appropriate media records which cannot be printed. *Examples include audio, video, and some web-sites.*

9 ADMINISTRATIVE FUNCTIONS

A level of organisational change is normal, and must be allowed for in the ERMS maintenance and system support facilities. An ERMS must also provide the Administrator with facilities to support events such as changing number of users, increasing demand on storage capacity, recovery from system failure and monitoring system errors.

Some of these facilities may be provided by the associated EDMS or database management system.

Requirements are listed in this chapter for general administration (section 9.1), system reporting (section 9.2) and for redaction of records (section 9.3).

9.1 General Administration

This section includes requirements for managing system parameters, backup and restore, system management and user administration.

Ref.	Requirement
9.1.1	The ERMS must allow Administrators, in a controlled manner and without undue effort, to retrieve, display and re-configure systems parameters and choices made at configuration time – for example, on elements to be indexed – and to re-allocate users and functions to user roles.
9.1.2	The ERMS must provide back-up facilities, and features to rebuild forward using restored back-ups and audit trails, while retaining system integrity. *In other words, the ERMS must include functionality to recreate the records and metadata to a known status, using a combination of restored back-ups and audit trails.*
9.1.3	The ERMS must provide recovery and rollback facilities in the case of system failure or update error, and must notify Administrators of the results. *In other words, the ERMS must allow Administrators to "undo" a series of transactions until a status of assured database integrity is reached. This is only required when error conditions arise.*
9.1.4	The ERMS must monitor available storage space, and notify Administrators when action is needed because available space is at a low level or because it needs other administrative attention.
9.1.5	The ERMS should monitor error rates occurring on storage media, and report to the Administrator any medium or device on which the error rate is exceeding a parameter set at configuration time. *In particular, this applies to optical media.*

Ref.	Requirement
9.1.6	The ERMS must allow Administrators to make bulk changes to the classification scheme, ensuring all metadata and audit trail data are handled correctly and completely at all times, in order to make the following kinds of organisational change: • division of an organisational unit into two; • combination of two organisational units into one; • movement or re-naming of an organisational unit; • division of a whole organisation into two organisations. When such a change is made, closed files must remain closed, retaining their references to the classification scheme before the change, and open files must either: • be closed, retaining their references to the classification scheme before the change, and cross-referenced to a new file in the changed scheme; or: • be referenced to the changed scheme, but clearly retaining all prior references to the classification scheme before the change. *Changes to organisational units described above may imply corresponding changes to the classification schemes of the units and their user populations.* *The term "bulk changes" implies that all classes, files, records affected can be processed with a small number of transactions, rather than needing to be processed individually.*
9.1.7	The ERMS must support the movement of users between organisational units.
9.1.8	The ERMS must allow the definition of user roles, and must allow several users to be associated with each role. *See also 4.1.3.*

9.2 Reporting

This section gives outline requirements only; it is not appropriate to attempt to reproduce here the requirements for a comprehensive report writing sub-system. In any implementation, requirements for the amount and complexity of reporting will be determined by the size, complexity and levels of change to the classification scheme, the amount and nature of the records, and the user base.

Ref.	Requirement
9.2.1	The ERMS must provide flexible reporting facilities for the Administrator. They must include, at a minimum, the ability to report the following: • numbers of files, volumes and records; • transaction statistics for files, volumes and records; • activity reports by user.
9.2.2	The ERMS must allow Administrators to enquire on and produce reports on the audit trail. These reports must include, at a minimum, reporting based on selected: • classes; • files; • volumes; • records; • users; • time periods.
9.2.3	The ERMS should allow Administrators to enquire on and produce audit trail reports based on selected: • security categories; • user groups; • other metadata.
9.2.4	The ERMS must be able to produce a report listing of files and volumes, structured to reflect the classification scheme, for all or part of the classification scheme.
9.2.5	The ERMS should include features for sorting and selecting report information.
9.2.6	The ERMS should include features for totalling and summarising report information.
9.2.7	The ERMS must allow Administrators to request regular periodic reports and one-off reports.
9.2.8	The ERMS should allow Administrators to restrict users' access to selected reports.

9.3 Changing, Deleting and Redacting Records

A basic principle is that records cannot normally be changed, and (except at the end of their life cycle in the ERMS) files and records cannot normally be deleted.

However, exceptions can arise; for example because of user error. This section defines these requirements.

Administrators may need to "delete" records to correct user errors (e.g. declaring records in the wrong file) or to meet legal requirements under data protection legislation. The action of deletion may mean one of two things:

- destruction (see 5.3.13 and 5.3.15);
- retention, accompanied by a notation in the record's metadata that the record is considered removed from records management control.

This ability to delete must be tightly controlled in order to protect the general integrity of the records. In particular, information about deletions must be stored in the audit trail, and trace of the deleted record(s) must remain in the affected folder(s).

Administrators sometimes need to publish, or make available, records which contain information which is still sensitive. This can result from data protection rules, security consideration, commercial risk, etc. For this reason, Administrators need to be able to remove the sensitive information, without affecting the underlying record. The process is referred to here as redaction, and the ERMS stores both the original record and the redacted copy, which is called here an "extract" of the record. Note that the need for extracts varies from country to country according to tradition.

Note that deletion and change are also discussed in chapter 5.

Ref.	Requirement
9.3.1	The ERMS must allow a default or option which prevents any record, once captured, from being deleted or moved by any Administrator or User. This means that any requirement for an Administrator to consider a record as "deleted" (as in 9.3.7) or "re-located" (as in 3.4.1) means that the record is marked appropriately; and in the case of re-location, a copy or pointer is inserted at the new location. *This requirement does not affect transfer or destruction of records in accordance with a retention schedule, as described in section 5.3.*
9.3.2	The ERMS should allow an option at configuration time, as an alternative to 9.3.1, that "deletion" of a record is implemented as destruction of that record.
9.3.3	The Administrator must be able to change the security category of individual records. *This is routinely required to reduce the level of protection given to records as their sensitivity decreases over time.*

Ref.	Requirement
9.3.4	The Administrator must be able to change the security category of all records in a file or class in one operation; the ERMS must provide a warning if any records are having their security category lowered, and await confirmation before completing the operation. *This is routinely required to reduce the level of protection given to records as their sensitivity decreases over time.*
9.3.5	Subject to support for 12.4.10 and 4.6.2, the Administrator must be able to change the security category of files.
9.3.6	The ERMS must record full details of any change to security category in the metadata of the record, volume or file affected.
9.3.7	The Administrator must be allowed to delete classes, files, volumes and records (subject to the option selected in 9.3.1). However, in the event of any such deletion the ERMS must: • record the deletion comprehensively in the audit trail; • produce an exception report for the Administrator; • delete the entire contents of a file or volume when it is deleted; • ensure that no documents are deleted if their deletion would result in a change to another record (for example if a document forms a part of two records – see 6.1.5 – one of which is being deleted); • highlight to the Administrator any links from another file, or record to a file or volume which is about to be deleted, requesting confirmation before completing the deletion; • maintain complete integrity of the metadata at all times (especially in view of 12.4.20 and 12.7.24). *This functionality is intended for exceptional circumstances only.*
9.3.8	The Administrator must be able to change any user-entered metadata element. Information about any such change must be stored in the audit trail. *This functionality is intended to allow Administrators to correct user errors such as data input errors, and to maintain user and group accesses.*
9.3.9	The ERMS must allow the Administrator to take a copy of a record, for the purposes of redaction. *This copy will be called an "extract" of the record in this specification.*

Ref.	Requirement
9.3.10	The ERMS should provide functionality for removing or hiding sensitive information from the extract, to include at least: • removal of individual pages of a multi-page image record; • addition of opaque rectangles to obscure sensitive names or words; • any other features required for video or audio formats if present. If the ERMS does not directly provide these facilities, it must allow for other software packages to do so. *It is essential that when these or any other redaction features are used, none of the removed or hidden information can ever be seen in the extract, whether on screen or when printed or played back, regardless of the use of any features such as rotation, zooming or any other manipulation.*
9.3.11	When an extract is created, the ERMS must record its creation in the record's metadata, including at least date, time, reason for creation and creator.
9.3.12	The ERMS should prompt the creator of an extract to assign it to a file.
9.3.13	The ERMS should store a cross reference (as in 11.1.18) to an extract in the same file and volume as the original record, even if that file volume is closed.
9.3.14	The ERMS must store in the audit trail any change made in response to the requirements in this section.

10 OTHER FUNCTIONALITY

This chapter contains requirements which may be relevant for functionality closely allied to electronic records management. It covers requirements for the management of physical records within the ERMS, document management, workflow, electronic signatures and other authentication mechanisms.

Note that this specification does not address the need to maintain physical records. Such a need may or may not exist, according to the legislative and regulatory environment; where there is such a need, care needs to be taken to preserve integrity and usability of electronic and physical records taken as a whole. These issues should be addressed by appropriate organisational policies.

In each case, requirements are presented at a high level. As they do not define the core functions of an ERMS, these requirements are deliberately indicative rather than complete.

The sections in this chapter list requirements for the following areas:

- management of non-electronic records (section 10.1);
- hybrid file retention and disposal (section 10.2);
- document management (section 10.3);
- workflow (section 10.4);
- electronic signatures (section 10.5);
- encryption (section 10.6);
- electronic watermarks etc. (section 10.7);
- interoperability and openness (section 10.8).

10.1 Management of Non-electronic Records

An organisation's records repository may contain records on paper and on other media such as videos, audiocassettes as well as electronic records. These are referred to as "physical files". The ERMS should be able to register physical files under the same classification scheme as the electronic records, and provide for the management of "hybrid files" of electronic and physical records.

Ref.	Requirement
10.1.1	The ERMS must be able to define in the classification scheme physical files and volumes, and must allow the presence of physical records in these volumes to be reflected and managed in the same way as electronic records.

Ref.	Requirement
10.1.2	The ERMS must define in the classification scheme files which (logically) contain both electronic and physical records, and must allow both kinds of record to be managed in an integrated manner. *These files are referred to as "hybrid files" in this specification. In practice, hybrid files will consist of an electronic file and a physical file.*
10.1.3	The ERMS must allow a physical file which is associated as a hybrid with an electronic file to use the same file title and numerical reference code, but with an added indication that it is a hybrid physical file.
10.1.4	The ERMS must allow a different metadata element set to be configured for physical files and electronic files; physical file metadata must include information on the physical location of the physical file (see 12.5.7).
10.1.5	The ERMS should support tracking of physical files by the provision of check-out, check-in and bring forward (also referred to as bring up) facilities which reflect the current location of the file.
10.1.6	The ERMS must ensure that retrieval of a hybrid file retrieves the metadata for both electronic and paper records associated with it.
10.1.7	Where files have security categories, (see 4.6) the ERMS should ensure that a hybrid physical file is allocated the same security category as an associated hybrid electronic file.
10.1.8	The ERMS must include features to control and record access to physical files, including controls based on security category, which are comparable to the features for electronic files (as defined in chapter 4).
10.1.9	The ERMS should support the printing and recognition of bar codes, or should support other tracking systems to automate the data entry for tracking physical file movements.

10.2 Hybrid File Retention and Disposal

Ref.	Requirement
10.2.1	The ERMS must support the allocation of retention schedules to every physical file in the classification scheme. The schedules must function consistently with scheduling for electronic files, notifying the Administrator when the disposal date is reached, but taking account of the different processes for destruction or archiving for paper and electronic records.
10.2.2	The ERMS must support the application of the same retention schedule to both the physical and electronic files which make up a hybrid file.
10.2.3	The ERMS must be able to apply any review decision made on a hybrid electronic file to a hybrid physical file with which it is associated.

Ref.	Requirement
10.2.4	The ERMS must alert the Administrator to the existence and location of any hybrid physical file associated with a hybrid electronic file which is to be exported or transferred.
10.2.5	The ERMS must be able to record in the audit trail all changes made to the metadata references to physical or hybrid files and records.
10.2.6	The ERMS should support the application of a review decision taken on a group of files to any physical files within that group, by notifying the Administrator of necessary actions to be taken on the physical files.
10.2.7	The ERMS should be able to export and transfer metadata of physical records and files.
10.2.8	The ERMS should be capable of offering check-out and check-in facilities for physical files profiled in the system, in particular enabling the ability to record a specific user or location to which a physical file is checked-out, and to display this information if the physical file is requested by another user. *Subject to the terms of security set out in section 4.6.*
10.2.9	The ERMS should be capable of offering a bring forward facility for physical files profiled in the system, enabling a user to enter a bring forward or reserve date for a physical file, and generating a consequent message for transmission to the current holder of that file or the Administrator, according to configuration. *Subject to the terms of security set out in section 4.6.*

10.3 Document Management

Electronic Document Management Systems – EDMS – are widely used in organisations to provide management and control over electronic documents. Many EDMS functions and facilities overlap with ERMS. EDMS would typically includes indexing of document, storage management, version control, close integration with desktop applications and retrieval tools to access the documents. Some ERMS systems provide full EDMS capability, others a subset. Conversely some EDMS have incorporated core record management functions.

By way of clarification, the following table shows typical differentiators.

An EDMS…	**An ERMS…**
• allows documents to be modified and/or to exist in several versions;	• prevents records from being modified;
• may allow documents to be deleted by their owners;	• prevents records from being deleted except in certain strictly controlled circumstances;

An EDMS…	An ERMS…
• may include some retention controls;	• must include rigorous retention controls;
• may include a document storage structure, which may be under the control of users;	• must include a rigorous record arrangement structure (the classification scheme) which is maintained by the Administrator;
• is intended primarily to support day-to-day use of documents for ongoing business.	• may support day-to-day working, but is also intended to provide a secure repository for meaningful business records.

The rest of this section sets out key requirements to be considered in provision of an integrated ERMS/EDMS solution. The requirements apply only where EDMS facilities are part of the solution.

Ref. **Requirement**

10.3.1 Where an EDMS is part of an ERMS, or is tightly integrated with an ERMS, the EDMS must be able to capture automatically electronic documents arising in the course of business and pass them to the ERMS registration process.

10.3.2 The ERMS with document management facilities must be able to:

- capture an electronic record in one process;
- register an electronic document and complete the capture at a later time.

10.3.3 Users should be able to register a document from within the EDMS or the application integrated with the EDMS.

This requirement is especially important where the EDMS/ERMS is used in a general office environment. It may be viewed as mandatory in many cases.

10.3.4 The user in EDMS, or in the application integrated with the EDMS, must be able to transfer adroitly to and from ERMS to register the document as a record from within the EDMS.

10.3.5 The ERMS with document management facilities must be able to acquire metadata elements directly from the document-generating application, and allow additional metadata elements to be completed by the user.

For example, the time of creation and user who created a document, and metadata identifiable from structured fields within documents if these exist, such as date and subject.

10.3.6 The ERMS must be capable of adding interfaces to new EDMS applications as these are brought into use by the organisation.

Ref.	Requirement
10.3.7	The ERMS with document management facilities should be able to manage electronic documents (which have not been registered as records) in the context of the same classification scheme and access control mechanisms as electronic records.
10.3.8	Where an EDMS is part of an ERMS, or is tightly integrated with an ERMS, the facilities for maintaining the classification scheme should be integrated.
10.3.9	The ERMS with document management facilities should be capable of managing versions of an electronic document as separate but related entities, while maintaining the link between them.
10.3.10	The EDMS should be able to restrict users to viewing: • only the latest version of a document; • all or selected versions of a document; • versions that have been captured or registered as records; the choice to be made at configuration time.
10.3.11	The ERMS with document management facilities should be able to interface with related packages, including image processing and scanning systems, and workflow systems whilst retaining full control of existing electronic records.
10.3.12	The ERMS must be able to copy the contents of an electronic record, in order to create a new and separate electronic document, while ensuring retention of the original record intact. *For example, a user may copy a record in order to send a copy to a recipient who is not a user of the ERMS. This copy may or may not be declared as a fresh record according to the context.*

10.4 Workflow

The Workflow Management Coalition (WfMC) – an international association for developing workflow standards and interworking of different workflow systems – defines workflow as "The automation of a business process, in whole or part, during which documents, information or tasks are passed from one participant to another for action, according to a set of procedural rules." In this definition, a "participant" can be a user, a work group (i.e. a team), or a software application.

The requirements in this section apply only where the ERMS includes workflow features. They cover both basic routing functions and more sophisticated workflow facilities, which may be provided by integrating a third party workflow product with the ERMS.

Workflow technologies transfer electronic objects between participants under the automated control of a program. In the context of ERMS, workflow is used to move electronic records between users and departments. It is commonly used for:

- managing critical processes or tasks such as registration and disposition procedures of files or records;
- checking and approval of records before registration;
- routing records or files in a controlled way from user to user for specific actions e.g. check document, approve new version;
- notifying users of the availability of records;
- distribution of records;
- publishing of records on the World Wide Web.

The capability of workflow systems vary from simple routing (such as checking and approving of a document before registration) through to handling high volume transactions with the handling of exception cases, and reporting on system and individual performance.

Ref.	Requirement
10.4.1	The ERMS workflow feature must provide workflows which consist of a number of steps, each step being (for example) movement of a record or file from one participant to another for action.
10.4.2	The ERMS should not practically limit the number of steps in each workflow.
10.4.3	The ERMS workflow must provide a function to alert a user participant that a file or record(s) have been sent to the user's electronic "in tray" for attention and specify the action required.
10.4.4	The ERMS workflow must allow the use of e-mail for a user to notify other users of records requiring their attention. *This implies integration to an existing e-mail system rather than a standalone or proprietary e-mail system.*
10.4.5	The ERMS workflow feature must allow pre-programmed workflows to be defined and maintained by the Administrator.
10.4.6	The ERMS workflow feature must prevent pre-programmed workflows from being changed by users other than the Administrator, or by approved users authorised by the Administrator.
10.4.7	The Administrator should be able to designate that individual users are able to reassign tasks/actions in a workflow to a different user or group. *A user may wish to send a file or record to another user because of the record content or the assigned user is on leave.*
10.4.8	The ERMS workflow feature must record all changes to pre-programmed workflows in the audit trail.

Ref.	Requirement
10.4.9	The ERMS workflow feature must record the progress of a record or file through a workflow so that users can determine the status of a record or file in the process.
10.4.10	The ERMS must not practically limit the number of workflows which can be defined.
10.4.11	The ERMS workflow feature should manage the files and records in queues which can be examined and controlled by the Administrator.
10.4.12	The ERMS workflow feature should be capable of letting participants view queues of work addressed to them and select items to be worked on.
10.4.13	The ERMS workflow feature should provide conditional flows depending on user input or system data. *In other words, flows which take the record or file to one of a number of participants depending on a condition decided by one of the participants. For example, a flow may take a record to either a credit control participant or an order consolidation section, depending on input from a sales supervisor; or the flow may depend on the value of an order, as computed by the system.*
10.4.14	The ERMS workflow feature should provide a reminder, or bring-forward, facility for files and records.
10.4.15	The ERMS workflow feature should allow users to interrupt a flow (i.e. to suspend it) temporarily in order to be able to attend to other work.
10.4.16	The ERMS workflow feature must recognise as “participants” both individuals and work groups.
10.4.17	Where the participant is a work group, the ERMS workflow feature should include a facility to distribute incoming items to group members in rotation, or on a member’s completion of the current task, to balance team members’ workloads.
10.4.18	The ERMS workflow feature should include the ability to prioritise items in queues.
10.4.19	The ERMS workflow feature should include “rendezvous” processing. *This requires the workflow to be paused to await the arrival of a related electronic document or record. When the awaited item is received, the flow resumes automatically.*
10.4.20	The ERMS workflow feature should be able to associate time limits with individual steps and/or process in each flow, and report items which are overdue according to these limits.
10.4.21	The ERMS workflow feature should allow the receipt of electronic documents to trigger workflows automatically.
10.4.22	The ERMS workflow feature must provide comprehensive reporting facilities to allow management to monitor volumes, performance and exceptions.

10.5 Electronic signatures

Electronic signatures (sometimes referred to as digital signatures) are sequences of characters which, when used with sophisticated secure algorithms procedures and "keys" (a long string of digits analogous to a password), can be used to confirm the integrity of a record, or to authenticate the identity of the sender of a record. An example of a widely-recognised electronic signature algorithm is MD5.

The wide adoption by organisations of e-mail and the World Wide Web has increased the number of documents that are moved internally and most significantly externally in relatively uncontrolled environments. The use of electronic signatures for authentication and integrity confirmation is becoming widely adopted.

The requirements in this section apply only where there is a requirement to manage records bearing electronic signatures. At time of writing, electronic signatures are effected by newly emerging technologies, still subject to change and uncertainty. Users of this specification should confirm requirements and implications for long-term storage with appropriate experts.

Ref.	Requirement
10.5.1	The ERMS must be able to retain the information relating to electronic signatures, encryption and details of related verification agencies.
10.5.2	The ERMS should have a structure which permits the easy introduction of different electronic signature technologies. *This is especially valuable given the changes occurring in this area.*
10.5.3	The ERMS should be capable of checking the validity of an electronic signature.
10.5.4	The ERMS must be able to retain and preserve as metadata, details about the process of verification for an electronic signature, including: • the fact that the validity of the signature was checked; • the Certification Authority with which the signature has been validated; • the date and time that the checking occurred.
10.5.5	The ERMS should be capable of checking the validity of an electronic signature at the time of capture of the record.
10.5.6	The ERMS should include features which allow the integrity of records bearing electronic signatures to be maintained (and to prove it has been maintained), even though an Administrator has changed some of its metadata, but not the content of the record, after the electronic signature was applied of the record. *The way in which this might be achieved is not prescribed.*

Ref.	Requirement
10.5.7	The ERMS should be able to store with the electronic record: • the electronic signature(s) associated with that record; • the digital certificate(s) verifying the signature; • any confirming counter-signatures appended by the certification authority in such a way that they are capable of being retrieved in conjunction with the record, and without prejudicing the integrity of a private key.

10.6 Encryption

Encryption is the process of applying a complex transformation to an electronic object so that it cannot be rendered by an application in a readable or understandable form unless the corresponding decryption transformation is applied. This can be used to secure electronic objects, by use of transformations which require the use of secure electronic key codes.

The requirements in this section apply only where there is a requirement to manage records which are encrypted.

Ref.	Requirement
10.6.1	Where an electronic record has been sent or received in encrypted form by a software application which interfaces with the ERMS, the ERMS must be capable of restricting access to that record to users listed as holding the relevant decryption key, in addition to any other access control allocated to that record.
10.6.2	Where an electronic record has been transmitted in encrypted form by a software application which interfaces with the ERMS, the ERMS should be able to keep as metadata with that record: • the fact of encrypted transmission; • the type of algorithm; • the level of encryption used.
10.6.3	The ERMS should be able to ensure the capture of encrypted records directly from a software application which has an encrypting capability, and restrict access to those users listed as holding the relevant decryption key.

Ref.	Requirement
10.6.4	The ERMS should allow encryption to be removed when a record is imported or captured. *This feature may be desired in some large scale record archives which have a requirement for long-term access (because encryption etc. is likely to reduce the ability to read records in the long term). In this case, the organisation would rely on audit trail or similar information to prove that the encryption etc. had been present but has been removed. In other environments, this feature may be undesirable from a legal point of view.* *See 5.3 for more details on Transfer and Importing.*
10.6.5	The ERMS should have a structure which permits different encryption technologies to be introduced easily.

10.7 Electronic Watermarks etc.

Electronic watermarks can used to mark an electronic image with provenance or ownership information. They superimpose on the image bitmap a complex visible or invisible pattern which can only be removed by use of an algorithm and a secure key. Similar technologies can be applied to digitised sounds and moving pictures. Watermarks typically are used to protect intellectual property.

The requirements in this section apply only where there is a requirement to manage records which bear an electronic watermark or some comparable technological control.

Ref.	Requirement
10.7.1	The ERMS must be capable of storing records bearing electronic watermarks, and of storing with them information about the watermark.
10.7.2	The ERMS should be able to retrieve information stored in electronic watermarks.
10.7.3	The ERMS should have a structure which permits different watermarking technologies to be introduced easily.

10.8 Interoperability and Openness

The requirements in this section are especially relevant to environments which require several ERMSs to communicate, for example large corporations or distributed government functions.

Ref.	Requirement
10.8.1	The ERMS should be able to inter-operate with other electronic records management systems.
10.8.2	The ERMS should be able to update other corporate systems.
10.8.3	The ERMS should be able to inter-operate with other applications. *The nature of the inter-operation will need to be specified for each application.*
10.8.4	The ERMS should be able to process in real time transactions generated by other external application systems.

11 NON-FUNCTIONAL REQUIREMENTS

Some of the attributes of a successful system cannot be defined in terms of functionality. In practice, *non-functional* requirements are important to success. While non-functional requirements often are difficult to define and measure objectively, it is nevertheless valuable to identify them so that they can be considered, at least at a high level. Accordingly, several are generic to many kinds of IT system.

In addition, users of this specification will need to consider their needs in relation to current technical and operational standards, and in relation to the ERMS supplier's support services including documentation, training and consultancy.

Organisations will need to add their own requirements in these areas, depending on their size and structure, physical characteristics and current technical operating environment. This section is intended as a checklist of aspects which users will need to consider when developing their requirements, to be added to the generic requirements given in earlier sections.

Some of the Example Requirements use angled brackets to indicate that the specification user needs to enter a quantified value or some other application-specific information. For example,

<xx minutes/hours>

means that the specification user should enter a length of time, probably measured in minutes or hours, to suit the specific requirement. Similarly,

<4 seconds>

means that the specification user should specify a time interval; 4 seconds is suggested as a starting point, for consideration.

The sections in this chapter list requirements for the following areas:

- ease of use (section 11.1);
- performance and scalability (section 11.2);
- system availability (section 11.3);
- technical standards (section 11.4);
- legislative and regulatory requirements (section 11.5);
- outsourcing and third party management of data (section 11.6);
- long term preservation and technology obsolescence (section 11.7).

11.1 Ease of Use

Ease of use is especially important. If an ERMS is not considered, by its users, easy to use, its implementation may fail.

Users of this specification must consider ease of use when specifying an ERMS. Consideration must include the degree of ease of use required, and how it is to be specified. This will depend on the kinds of user for whom it is intended, and the amount of training. Examples of requirements for ease of use are listed below.

Ref.	Example Requirement
11.1.1	The ERMS must provide online help throughout the ERMS.
11.1.2	The online help in the ERMS should be context-sensitive.
11.1.3	All error messages produced by the ERMS must be meaningful, so that they can be appropriately acted upon by the users who are likely to see them. *Ideally, each error message will be accompanied by explanatory text and an indication of the action(s) which the user can take in response to the error.*
11.1.4	The ERMS must employ a single set of user interface rules, or a small number of sets. These must be consistent with the operating system environment in which the ERMS operates. *The rules should be consistent with other mainstream applications already installed.*
11.1.5	The ERMS must be able to display several records simultaneously (subject to any contrary requirement implied by 11.1.4).
11.1.6	Where the ERMS uses on-screen windows, each should be user-configurable (subject to any contrary requirement implied by 11.1.4).
11.1.7	The ERMS user interface must be suitable for users with special needs; that is, compatible with specialist software that may be used and with appropriate interface guidelines. *The following Guidelines which may be useful in this context are listed in Annex 7 part 3:* • *SPRITE-S^2 initiative ACCENT – Accessibility in ICT Procurement;* • *W3C Web Content Accessibility Guidelines;* • *Microsoft Official Guidelines for User Interface Developers and Designers.*
11.1.8	The ERMS must provide end user and Administrator functions which are easy to use and intuitive throughout (as may be assessed by a panel of typical users).
11.1.9	Where the ERMS includes the use of windows, it must allow users to move, re-size and modify their appearance, and to save modifications in a user profile.

Ref.	Example Requirement
11.1.10	The ERMS should allow users to select sound and volume of audio alerts, and to save modifications in a user profile.
11.1.11	The ERMS must allow persistent defaults for data entry where desirable. These defaults should include: • user-definable values; • values same as previous item; • values derived from context, e.g. date, file reference, user identifier; as appropriate.
11.1.12	Frequently-executed ERMS transactions must be designed so that they can be completed with a small number of interactions (e.g. mouse clicks).
11.1.13	The ERMS should be closely integrated with the organisation's e-mail system in order to allow users to send electronic records and files electronically without leaving the ERMS.
11.1.14	Where requirement 11.1.13 is met, the ERMS should provide this by sending pointers to files and records rather than copies, whenever a file or record is sent to another user of the ERMS. *There will be exceptions to this such as a remote user that does not have consistent access to the central repository.*
11.1.15	Where the ERMS employs a graphical user interface, it must allow users to customise it. Customisation should include, but need not be limited to the following changes: • menu contents; • layout of screens; • use of function keys; • on-screen colours, fonts and font sizes; • audible alerts.
11.1.16	The ERMS should support user-programmable functions. *For example, user-definable macros; but see section 6.3 concerning self-modifying documents.*
11.1.17	Where users have to enter metadata from images of printed documents, the ERMS should provide features to allow the use of optical character recognition to capture metadata from the image (zoned optical character recognition).
11.1.18	The ERMS should allow users to define cross-references between related records, both within the same file and in different files, allowing easy navigation between the records.
11.1.19	The ERMS should include help on use of the classification scheme.

11.2 Performance and Scalability

Users of this specification should consider the extent to which the ERMS provides short response times (in line with user expectations), and is capable of serving the range of sizes of user population for which it is intended. Some considerations and example requirements are given below.

The response times experienced by users will depend on factors outside the ERMS, for example:

- network bandwidth;
- network utilisation;
- configuration and utilisation of various server resources.

This specification cannot address such external factors, other than to point out that they must not be ignored. Usually, tests in the live environment are needed to obtain a reliable view of performance.

Accordingly, these requirements should be interpreted with a standardised understanding of "response time". This standardised understanding will vary from environment to environment, depending on the status of the infrastructure. For example, if the ERMS is being specified for an existing infrastructure, it may be appropriate to specify response times in terms of the time between receipt of a keystroke at the server, and sending of the response. Alternatively, if the specification is for of a turnkey system to include servers and network, it may be appropriate to specify response times in terms of the time between a keystroke and display of the response on the workstation.

Users of this specification may also find it useful to refer to the European Commission Display Screen Equipment Directive (90/270/EEC) which refers to software performance.

Ref.	Example Requirement
11.2.1	The ERMS must provide adequate response times for commonly performed functions under standard conditions, for example: • 75% of the total anticipated user population logged on and active; • 100% of the anticipated total volume of documents managed by the system; • users performing a mix of transaction types at various rates; with consistency of performance over at least ten transaction attempts.

Ref.	Example Requirement
11.2.2	The ERMS must be able to perform a simple search within <3 seconds> and a complex search (combining four terms) within <10 seconds> regardless of the storage capacity or number of files and records on the system. *In this context, performing a search means returning a result list. It does not include retrieving the records themselves.*
11.2.3	The ERMS must be able to retrieve and display within <4 seconds> the first page of a record which has been accessed within the previous <xx> months, regardless of storage capacity or number of files/records on the system. *This requirement is intended to allow for rapid retrieval of frequently-used records, on the understanding that frequency of use is typically correlated with recent use. The timescale is to be inserted by the organisation, based on an evaluation of the time after which the heavy usage of records decreases.*
11.2.4	The ERMS must be able to retrieve and display within <20 seconds> the first page of a record which has not been accessed within the previous <xx> months, regardless of storage capacity or number of files/records on the system. *This requirement is intended to allow for cases where a form of hierarchical storage management is used, where records used infrequently are stored on slower media than more active records. The timescale is to be inserted by the organisation, based on an evaluation of the time after which the heavy usage of records decreases.*
11.2.5	The ERMS must allow a single implementation of the system to have an electronic record store of at least <xx gigabytes/terabytes> or <xx thousand/million> records, and to serve at least <xx hundred/thousand> users simultaneously. *Estimates of record and user population to be inserted by the organisation.*
11.2.6	It must be possible to expand the ERMS, in a controlled manner, up to at least <xx hundred /thousand> users while providing effective continuity of service.
11.2.7	The ERMS must support the above, including routine maintenance of: • user and group data; • access profiles; • classification schemes; • databases; • retention schedules; in the face of the anticipated levels of organisational change, without imposing undue systems/account administration overheads (see also chapter 9). *In cases where performance requirements are strict, it may be necessary to quantify the anticipated levels of organisational change.*

Ref.	Example Requirement
11.2.8	The ERMS be scaleable and must not have any features which would preclude use in small or large organisations, with varying numbers of differently-sized organisational units.

11.3 System Availability

In many environments, use of an ERMS and EDMS together will transform the use of IT systems. A major change is that users' dependence on the IT network will increase dramatically, because if the EDMS/ERMS becomes unavailable they may be unable to continue working. Accordingly, users of this specification who are procuring a system should make every effort to identify users' requirements for availability, and then to specify these for the procurement. Example requirements for maintenance are given below.

Ref.	Example Requirement
11.3.1	The ERMS must be available to users: • from <xx:00> to <xx:00>; • on <all weekdays/xxx days per year>.
11.3.2	The planned downtime for the ERMS must not exceed <xx> hours per <rolling three month period>. *The definition of "down" may depend on the infrastructure and architecture. For example, in some environments, a failure caused by server hardware will be considered as a failure of the ERMS; in other environments the failure of mainframe hardware will be considered as a different kind of failure, not attributable to the ERMS. A suitable definition needs to be agreed; as a starting point the following is proposed: "The ERMS is considered to be down if any users are unable to perform any normal ERMS function if this failure is attributed to any component of the ERMS other than the workstation."*
11.3.3	Unplanned downtime for the ERMS must not exceed <xx hours/minutes> per <rolling three month period>.
11.3.4	The number of incidents of unplanned downtime for the ERMS must not exceed <x> per <rolling three month period>.
11.3.5	In the event of any software or hardware failure, it must be possible to restore the ERMS to a known state (no older than the previous day's backup) within no more than <xx> hours of working hardware being available.

11.4 Technical Standards

The ERMS should comply with relevant de facto and de jure standards. Where possible, it is desirable that the ERMS should make use of open rather than proprietary specifications and formats.

Users of this specification will need to specify requirements for standards covering:

- hardware environment (e.g. server platforms, workstation environments);
- operating system environment (e.g. Microsoft Windows – NT4, 98, 2000 – MacOS, Unix);
- user interface industry standards (e.g. Microsoft Windows, Macintosh, X-windows, intranet browser);
- relational database (e.g. ODBC, OLE DB; possibly product, e.g. Oracle, Sybase);
- network protocols and operating system (e.g. TCP/IP, Ethernet type, Novell, Microsoft Windows NT Server);
- encoding at various levels (e.g. ASCII, Unicode ISO 10646, ISO 8859, Adobe PDF or other equivalent proprietary specifications);
- interchange standards (e.g. XML, HTML, SGML);
- application program interface and developer kits (e.g. COM, DCOM, CORBA).

When using this specification for procurement, it will be necessary to add further details of the technical environment, including all ERMS interfaces (e.g. legacy systems, office systems) and any plans for change.

Additionally, users of this specification will need to consider their requirements, in the light of their individual context, in the following areas of standards:

Ref.	Example Requirement
11.4.1	If a monolingual thesaurus is implemented with the ERMS, it should comply with standard ISO 2788, Guidelines for the establishment and development of monolingual thesauri.
11.4.2	If a multilingual thesaurus is implemented with the ERMS, it should comply with standard ISO 5964, Guidelines for the establishment and development of multilingual thesauri.

Ref.	Example Requirement
11.4.3	If the ERMS includes scanning of paper documents, the following standards should be complied with: • TWAIN and/or Isis scanner interfaces; • TIFF v6 image format with Group IV facsimile compression for bi-level images; • JPEG, PNG, GIF or other user-selectable format if colour or grey-scale images are supported. *If these standards are not complied with, an adequate reason should be sought.*
11.4.4	The ERMS must support the storage of records using file formats and encoding which are either de jure standards or which are fully documented.
11.4.5	The ERMS should conform to the search and retrieval and information exchange standards, including ISO 23950, Information retrieval – application service definition and protocol specification. *This standard is also referred to as ANSI Z39.50.*
11.4.6	If a relational database is used by the ERMS, it must conform to the SQL standard, ISO/IEC 9075, Information technology – database languages – SQL.
11.4.7	The ERMS should store all dates in a format compliant with ISO 8601, Data elements and interchange formats – Information interchange – Representation of dates and times.
11.4.8	The ERMS should store all country names in a format compliant with ISO 3166, Codes for the representation of names of countries.
11.4.9	The ERMS should store all language names in a format compliant with ISO 639, Codes for the representation of names of languages.
11.4.10	If the ERMS is to manage records in multiple languages or using non-English characters, it must be capable of handling ISO 8859-1 encoding.
11.4.11	If the ERMS is to manage records in multiple languages or using non-English characters, it should be capable of handling ISO 10646 encoding (Unicode).

11.5 Legislative and Regulatory Requirements

The ERMS must conform to legislative and regulatory requirements, which typically vary from region to region and between industries.

Note that this specification does not address the need to maintain physical records. Such a need may or may not exist, according to the legislative and regulatory environment; where there is such a need, care needs to be taken to preserve integrity and usability of electronic and physical records taken as a whole. These issues should be addressed by appropriate organisational policies.

The following requirements will require localisation.

Ref.	Example Requirement
11.5.1	The ERMS must conform to applicable standards for year 2000 compliance, and must process all dates correctly. *Some ERMS have to process dates covering an interval centuries long. Correct processing of all dates may include dates in several different centuries. An example of a statement which specifies this in more detail is reproduced in Annex 6.*
11.5.2	The ERMS must conform to locally-applicable standards for legal admissibility and evidential weight of electronic records.
11.5.3	The ERMS must comply with locally-applicable record management legislation.
11.5.4	The ERMS must not include any features which are incompatible with data protection or other legislation.
11.5.5	The ERMS must comply with <any relevant European, national or local regulatory requirements or code of practice for the industry, business function or government sector>. *This requirement is to be customised for specific environments.*

11.6 Outsourcing and Third Party Management of Data

Many organisations use service providers to store and manage records which have are no longer active (or have extremely low recall requirements) but which need to be retained for a legislative period demanded by legal/government stipulation, industry regulators or for long term preservation.

There is also an increasing use of Application Service Providers (ASP) to manage active records as well as an archive. Organisations send their documents or records — invoices, customer correspondence, mortgage application documents etc. — to be indexed and stored by the ASP. The documents are then available for viewing by the organisation's staff over the Internet or through a Wide Area Network.

The management of electronic records by a third party requires that the contract with the service provider has clearly defined procedures and controls in place to meet regulatory requirements, adhere to best practice for legal admissibility of electronic records, and meet the business demands of the client for access and availability.

The contract will need to include provisions that:

- the service provider's management must be to a standard at least as good as that of the client's management of internal records;

- the client will be able to recover the records from the service provider at a time in the future, and still be able to continue the management of the records to the organisation's standards and meet legal admissibility requirements.

This sub-section draws heavily on PD 0008 (see Annex 1 reference [5]), section 4.14 "Use of contracted services."

Ref.	Requirement
11.6.1	A contract must be agreed with the service provider that details the services that are to be used.
11.6.2	Details of the procedures for the transfer of records from the client to the service provider, and from the service provider to the client must be documented. *This may use communication links between the sites and automatically transfer files and records on a daily or regular basis. The client must be satisfied that the link between the two sites is secure and the protocols are in place to check all records are received, and reports produced.*
11.6.3	The service provider must be able to provide the client with copies of the audit trail of the processes for logging and storing of the records/files.
11.6.4	The service provider must demonstrate that facilities are in place so that the files/records and metadata stored can be easily transferred back to the client's ERMS without any loss of structure or content of the records. Also the service provider must have procedures in place to allow the client to transfer individual files and records.
11.6.5	The service provider must be able to provide ready access to the managed records by the client. The service provider must either deliver a rendition of the record, or the original record to the client to a contracted agreed time and price.
11.6.6	The service provider should be able to provide the client with the ability to request, view and print records and or files from the client's office. *This can be achieved, for example, by a network connection.*
11.6.7	The service provider should be able to provide the client with the ability to request on-line the downloading or transmitting of records and or files between the client's ERMS system and service provider's storage facility.
11.6.8	The client should be able to request reports on the records held by the service provider and details of retention schedules etc. This facility should be provided on-line from the client's offices.
11.6.9	Services specified in 11.6.6, 11.6.7 and 11.6.8 should: • have contracted response times and/or turnaround times; • operate in a secure environment.

Ref.	Requirement
11.6.10	The client should check that the proposed location of the work is acceptable and meets security criteria appropriate to the client's needs.
11.6.11	The client should check that the proposed procedures and storage management processes involve no greater risk to the records than the client's procedures. *The service provider will need to demonstrate that all the client's records are backed up and in the event of loss of the records they can be recovered to an contracted timescale.*
11.6.12	Where the security of the records is important, the client should check that the service provider will vouch for the trustworthiness of the operational staff. *It is an advantage if all employees of the service provider sign a confidentiality agreement as part of their conditions of employment.*
11.6.13	Each shipment of records to/from the client and the service provider should be accompanied by a control document stating the identity and number of records and files.
11.6.14	Third parties providing transportation services should be organisations that demonstrably meet the quality and reliability criteria of the client.

11.7 Long Term Preservation and Technology Obsolescence

This section addresses long term preservation. "Long term" is not defined precisely; but it is understood here to mean "for a period of more than ten years or so". In any organisation, the retention period should be determined by legislation and business needs. In some environments, this will mean several decades; in some archives it may extend to centuries. In either case, the time period is sufficiently long that approaches used routinely for shorter periods cannot be assumed to be appropriate.

Electronic records held for the long term face risks from three directions:

- media degradation;
- hardware obsolescence;
- format obsolescence.

These are discussed below. The discussions are followed by specific requirements. However, readers should note that this specification does not provide detailed requirements for all aspects of this issue; each organisation should develop and implement a strategy for the long-term preservation of its electronic records, much as is often the case for paper-based records.

In the discussion which follows, preservation of records implies preservation of the metadata and audit trails information which accompanies them.

Media Degradation

The risk from media degradation arises because all digital storage media have a limited lifetime. The lifetime varies from media to media, and varies also according to storage conditions (temperature, humidity and rates of change). As media reach, or exceed, their expected lifetime, the likelihood of read errors (that is, bits read incorrectly) increases dramatically. Most storage hardware has automatic error correction built into it; this can cope with a certain level of bit errors, effectively compensating for them. But eventually, the read errors become so numerous that the automatic error correction cannot cope; at this stage, records become irretrievably corrupt. The effect of this corruption depends on many factors, but can lead to individual records or whole discs, tapes etc. becoming unreadable.

The following precautions can be taken to avoid loss of information due to media degradation:

- ensure all media is stored, used and handled in suitable environmental conditions. As a general rule, the cleaner, cooler, dryer and more stable the environment, the longer the expected life. However, for specific media, the manufacturer's specifications must be followed (e.g. the environment must not be colder than a certain temperature; the media must, or must not, be periodically cleaned);

- routinely replace media (by copying information from them to fresh media) before the expected end of life;

- keep several copies of each record, and systematically compare copies according to a schedule; then replace any copy of a record which shows an unrecoverable error, and replace any piece of media which shows an unrecoverable error. This approach is typically used in specialist long-term data archives; it requires automated systems and retrieval hardware, further description of which are beyond the scope of this specification.

Hardware Obsolescence

Storage peripherals – tape drives, disc drives – have a limited market life. As they exceed this life, they typically require more maintenance, while at the same time becoming expensive to maintain and repair; eventually they become unrepairable for practical purposes. In some cases, sharing agreements can be reached with other users of similar or compatible equipment; but this is not sustainable indefinitely. At some point, information stored on obsolete devices, and not copied onto other media, may be lost permanently if the device fails.

The same problem arises with the computers which manage the applications and storage.

Clearly the strategy to avoid this risk is to monitor the status of the hardware, and to migrate the information to new, current media before obsolescence puts the

information at risk. In all cases, media and hardware should be chosen which have a good life expectancy; in other words, popular or "market leading" may be a better choice than new and state-of-the-art.

Format Obsolescence

Format obsolescence presents the most difficult problem for any period longer than a handful of decades.

The problem arises because the many software components involved in the processing "chain" between media and rendered information are constantly evolving. The components include:

- encoding standards;
- file formats;
- application software;
- database and other utility software;
- operating system software.

Their evolution is rapid, and different components evolve in different ways, at different rates. Some evolution retains compatibility with prior formats. However, some evolution does not retain compatibility – and this is especially true over periods longer than a handful of decades. It is not possible to avoid the evolution by "freezing" the configuration, because of the need to migrate to current hardware, as described above; new hardware frequently requires new software drivers, which in turn require a new operating system, and so on.

Currently, the following techniques are recognised:

- migration (converting information to new formats which can be accessed by current hardware and software);
- emulation (moving the information to new hardware but with a additional software component which emulates the old hardware, thus allowing execution of the old application software);
- technology preservation (continual maintenance of the original hardware; not practical in the long term);
- bundling of data and software (a theoretical approach which is immature at time of writing; see BS 7978 at Annex 7 part 1).

Although much research work is under way to minimise the risk, there is at time of writing no simple, generic method which will guarantee long term access to electronic records. Consensus is that migration and/or emulation are likely to be the safest options; in practice, both will require attention to preservation metadata – see below.

However, large-scale migrations are rarely free of problems; they can result in the loss of individual items, and they sometimes result in loss of functionality, detail, or some other characteristic.

Likewise, large-scale, long-term emulation is not well-understood. It also has risks of loss of functionality and other characteristics.

The difficulties are compounded by the prospect of repeated migrations or emulations. Nobody can predict the nature of the migrations or emulations which may be required; and nobody can predict the consequences of repeated migrations or of several "layers" of emulation.

The most appropriate strategy is to hold information only in widely-accepted, stable, open formats (i.e. formats which are comprehensively documented in publicly-available specifications) which have a long expected life. As with hardware, this suggests "market leading" rather than unproven or state-of-the-art; and it suggests proprietary formats should be avoided where their specifications are not publicly available. There is also an implication that the organisation will need some expertise when selecting formats.

The volatility of the multimedia market, and of the proprietary formats it uses, makes multimedia an area of particular concern.

As this problem requires an organisation-specific response, more detailed discussion at the generic level of this specification would not be helpful. However, it is appropriate to point out that each approach involves expense – in hardware, software, data preparation and conversion, and management – and yet none will preserve access unless a strategy for long-term preservation is implemented before accessibility becomes problematic. In other words, long-term preservation requires the preventive expenditure of amounts which may grow to be large; this is similar in concept to the preservation of paper archives, save that in some cases the expenditure will be larger. Where long term preservation is required, it is therefore essential that senior management is committed to the ongoing effort and expense required to safeguard access. Further sources of information are given in Annex 7 part 4.

Preservation Metadata

It is essential that preservation metadata be stored with the records when long term storage is needed. This metadata provides information beyond the scope of the metadata specified in this specification, such as information about the technical environment, about the software used to create a record and about software needed to render a record – and all its components. Where the preservation period is unlimited, the number of metadata elements required becomes large. Several research projects in Europe, North America and Australia are developing metadata frameworks at time of writing; their results are becoming available through the internet. The complex nature of the preservation metadata has led to the

development of the OAIS reference model (see Annex 7 part 4), which can be used to structure the metadata for preservation purposes.

Specific Requirements

The requirements in this section are proposed as a minimum technical requirement where long-term storage is envisaged. However, as indicated above, management commitment is equally important.

Ref.	Requirement
11.7.1	The ERMS storage media must be used and stored in environments which compatible with desired/expected life, and which is within the tolerance of the media manufacturer's specification. *In some cases a standard such as BS 4783 (see Annex 7 part 1) can be cited.*
11.7.2	The ERMS should include features for the automated periodic comparison of copies of information, and the replacement of any copy found to be faulty, to guard against media degradation.
11.7.3	The ERMS must allow the bulk conversion of records (with their metadata and audit trail information) to other media and/or systems in line with the standards relevant for the format(s) in use.
11.7.4	The ERMS supplier must have a demonstrable programme in place for upgrades to the ERMS technology base that allows for the existing information to continue to be accessed without changes to the content.
11.7.5	The ERMS should use only widely-accepted standards which are the subject of open and publicly available specifications for encoding, storage and database structures.
11.7.6	If the ERMS uses any proprietary encoding or storage or database structures, these must be fully documented, with the documentation being available to the Administrator. *Note that this implies it may not be sufficient for the supplier to retain a copy of the documentation; in the timescale being considered, the stability of the supplier is not certain. It may therefore be desirable for a copy of this documentation to be lodged with the user organisation or with a neutral third party.*
11.7.7	The ERMS should be able to manage a range of preservation metadata elements for the records and their component parts. *See 12.7.13.*

12 METADATA REQUIREMENTS

Metadata includes, in the context of this specification, indexing information and also other data such as access restriction information. A formal definition is given in the glossary, section 13.1.

This chapter is arranged differently from preceding chapters; see section 12.2.

12.1 Principles

It is not possible to define all the metadata requirements for all possible kinds of ERMS implementation. Different kinds of organisations and applications have particular needs and traditions which vary enormously. For example, some organisations will need indexing which is focussed on account names and transaction dates while others will need strict hierarchical numbering; some will need volumes which relate to financial years while others will not; some will need access controls for security reasons, others for intellectual property reasons, and so on.

This chapter of the MoReq specification therefore suggests minimum requirements which are intended to be generic, but which are intended for customisation. These minimum requirements include lists of specific metadata elements which the ERMS must be able to capture and process.

Almost any prospective ERMS can be configured with sufficient fields to support the metadata elements listed below; however, this alone is insufficient. It is important that:

- the ERMS must use the metadata elements to enable and support the functionality defined in the remainder of this specification (see 12.1.2);
- the ERMS must include features supporting validation, inheritance and default value rules when capturing the metadata elements.

Ref.	Requirement
12.1.1	The ERMS application must not present any practical limitation on the number of metadata elements allowed for each item (e.g. file, volume, record). *The definition of "practical limitation" will vary according to the application. For example, small organisations with a small classification scheme may not need as many metadata elements as large organisations with a large classification scheme.*

Ref.	Requirement
12.1.2	Where the contents of a metadata element can be related to the functional behaviour of the ERMS, then the ERMS must use the contents of that element to determine the functionality. *For example, if the ERMS stores security categories of records and also stores the security clearance of users, then it must use the latter to determine whether a user can or cannot access a record. If the ERMS only stores the clearances and categories as text fields which are not used to control access, this requirement is not met.* *Note that this is a general requirement which stretches across many metadata elements; this specification does not attempt to identify all cases in which this is relevant.*
12.1.3	The ERMS must allow different sets of metadata elements to be defined for different kinds of electronic record at configuration time. *For example, records which are scanned images will need metadata relating the scanning and indexing processes; invoices will need account number metadata; correspondence will need multi-value recipient metadata fields.*
12.1.4	The ERMS must allow the Administrator to define at configuration time whether each metadata element is mandatory or optional and whether it is searchable.
12.1.5	The ERMS must support at least the following metadata element formats: • alphabetic; • alphanumeric; • numeric; • date; • logical (i.e. YES/NO, TRUE FALSE).
12.1.6	The ERMS should support metadata element formats, definable by the Administrator, which consist of combinations of the formats in 12.1.5. *For example, an application might have a reference number in the format nnnnn/aa-n.*
12.1.7	The ERMS must support date formats defined in ISO 8601 for all dates.
12.1.8	At time of configuration, the ERMS must allow definition of the source of data for each metadata element. *Possible sources are described in requirements 12.1.9, 12.1.10, 12.1.11, 12.1.12.*

Ref.	Requirement
12.1.9	The ERMS must support the ability to extract metadata elements automatically from records when they are captured. *There are some applications where this may not be mandatory. The requirement is considered mandatory here because it is especially important in many cases. Examples are the automatic extraction of dates, titles, recipient names and reference numbers from word processed documents or structured transaction documents such as invoices.*
12.1.10	The ERMS must allow the Administrator to specify which metadata elements are to be entered and maintained by keyboard entry or from a pull-down list.
12.1.11	The ERMS should allow for the values of metadata to be provided automatically from the next higher level in the classification scheme hierarchy. *For example, for a volume, the value of some of the metadata elements must be inherited from its parent file; and for a record, the value of some metadata may be inherited from the volume into which it is stored.*
12.1.12	The ERMS should allow values of metadata to be obtained from lookup tables or from calls to other software applications. *For example, the ERMS might provide name and post code to an addressing application which then returns a street name to be used as metadata.*
12.1.13	The ERMS must support validation of metadata when the metadata is entered by users, or when it is imported. The validation must use at least the following mechanisms: • format of the element contents; • range of values; • validation against a list of values maintained by the Administrator; • valid classification scheme reference. *An example of format validation is that the contents are all numeric, or are in a date format (consistent with 12.1.5).* *An example of range format validation is that the contents fall in the range between 1 January 1999 and 31 December 2001.* *An example of validation against a list of values is verifying that an export destination is present on a list.*

Ref.	Requirement
12.1.14	The ERMS should support validation of metadata elements using check digit algorithms. *For example, files may be identified by a sixteen-digit credit card number, of which the last digit is a check digit computed from the other fifteen digits using the mod 10 algorithm.* *Provision of an application program interface for this feature, allowing organisations to introduce their chosen algorithm, should normally be considered acceptable.*
12.1.15	The ERMS must, where required, support validation of metadata using calls to another application (e.g. to a personnel system to check whether a personnel number has been assigned, or to a post code database system).
12.1.16	Where metadata element values are entered manually, the ERMS must support persistent default values which are user-definable. *A persistent default appears as the default in the data entry field for each item in succession until it is changed by a user. Once changed, the new value remains, i.e. becomes persistent.*
12.1.17	The ERMS should allow configuration such that any metadata element can be used as a search field in a non-structured search (e.g. a free text search).
12.1.18	Where a metadata element is stored in date format, the ERMS should allow searches which recognise the value of the date. *For example, the ERMS should support searches in a date range. It is not sufficient for the date to be stored as a text field.*
12.1.19	Where a metadata element is stored in numeric format, the ERMS should allow searches which recognise the value of the number.
12.1.20	The ERMS must restrict the ability to make changes to metadata values as defined in the matrix in section 13.4.
12.1.21	The ERMS must allow reconfiguration of metadata sets by the Administrator, and must record such in the audit trail. *For example, it may be necessary to add a new data element such as "Department Identifier" to some document types following an organisational change.*
12.1.22	The ERMS should be able to acquire metadata from: • the document-creating application package or operating system or network software; • the user at the time of capture or declaration; • rules defined at configuration time for generation of metadata by the ERMS at the time of declaration.

Ref.	Requirement
12.1.23	The ERMS must be able to prevent any amendment of metadata generated directly from other application packages, the operating system or the ERMS, for example, e-mail transmission data.
12.1.24	The ERMS must prevent the contents of metadata fields specified at configuration time from change.

12.2 Organisation of the Remainder of this Chapter

The remainder of this chapter lists generic functional metadata elements for each level of the filing hierarchy:

- classification scheme;
- file;
- file volume;
- record.

The lists of metadata requirements are formatted differently from the tables in other chapters. The arrangement is columnar as before; the new column headings are described here.

Ref.

A requirement reference number.

Metadata Elements

The ability of the ERMS to include each metadata element is shown as one requirement.

The requirements all start with "The ERMS must…" or "The ERMS should…" As in the rest of this specification, the word "must" indicates a mandatory requirement and the word "should" indicates an optional requirement.

For simplicity, the lists do not include values which are inherited from higher levels in the hierarchy. So, for example, file volumes naturally inherit metadata such as name, reference number etc. from their parent files; but this is not shown here.

Occurs

For each element, the requirement includes the number of occurrences of that element which must be supported by the ERMS (technically referred to as "cardinality"). The number of occurrences is shown as follows:

1 indicates that the metadata element must occur once for each item (e.g. file, volume 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 : Each ERMS user must have at least one, but maybe more than one *role*.

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 file volume or record, and metadata elements that may never be required for a specific item.

Example : An *electronic file close date* will not be present until the file is closed, but must be present exactly once when the file has been closed.

Example : A *record protective marking security category* may be allocated, or may never be allocated, to an electronic record; but if allocated, 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 file may not be present at all, or may occur one or more times, depending on the review history of the file.

Req.

Finally, each metadata element is cross-referenced to a requirement which gives rise to it. Thus this section can be used to understand a requirement which gives rise to a need for a metadata element, so that the element can better be understood.

In some cases, several requirements imply a metadata element; in these cases, they are not all listed. It is therefore important to note that this section cannot be used to determine all the requirements which refer to a given metadata element.

An exception is made for “user-defined metadata” elements. The requirements for these are not cross-referenced.

In the electronic version of this specification, the requirement number is a hyperlink to the requirement.

An entry of “N/A” indicates “not applicable”.

12.3 Classification Scheme Metadata Elements

The ERMS should support the following for each classification scheme:

Ref.	Metadata element	Occurs	Req.
12.3.1	Name. *This may be the name of the organisational unit (department, section etc.) responsible for the classification scheme.*	0-1	3.1.8
12.3.2	Identifier.	0-1	3.1.8
12.3.3	Description.	0-1	3.1.8
12.3.4	User-defined metadata elements.	0-n	N/A
	Note: at least one of 12.3.1, 12.3.2, 12.3.3 must be present.		

12.4 Class and File Metadata Elements

The ERMS must support the following for each class and file:

Ref.	Metadata element	Occurs	Req.
12.4.1	Identifier.	1	3.2.2 7.1.1
12.4.2	Name.	1	3.2.2 7.1.1
12.4.3	Descriptive keywords.	0-n	3.2.8
12.4.4	Description.	0-1	3.2.2
12.4.5	Date opened.	1	3.2.4
12.4.6	Date closed.	1	3.3.4
12.4.7	Person or post responsible for maintenance.	1	4.1.1 4.1.7
12.4.8	User group access rights. *Information about which user groups can access the file or class, and the kinds of access they are allowed.*	0-n	4.1.1 4.1.7
12.4.9	User access rights. *Information about which users can access the file or class, and the kinds of access they are allowed.*	0-n	4.1.1 4.1.7
12.4.10	Security category.	0-1	4.6.2

Ref.	Metadata element	Occurs	Req.
12.4.11	If requirement 12.4.10 is supported, security category history, i.e. for each previous category: • category; • dates of change; • reason for change; • user responsible for change.	0-n	9.3.6
12.4.12	Rule(s) for closing volumes.	1-n	3.4.8
12.4.13	If the ERMS is used to manage paper files, details of the related paper file (or an indication of the existence of a hybrid file). *Not required for classes.*	0-1	10.1.1
12.4.14	User-defined metadata elements.	0-n	N/A
12.4.15	Deletion date.	0-1	9.3.7
12.4.16	Deleted by.	0-1	9.3.7
12.4.17	Retention schedule.	0-n	5.1.4 5.1.5
12.4.18	Classification history.	0-n	3.4.4 9.1.6
12.4.19	Reason for re-classification.	0-n	3.4.5

The ERMS should support the following for each class and file:

Ref.	Metadata element	Occurs	Req.
12.4.20	Links to related files. *Not required for classes.*	0-n	3.4.11
12.4.21	Other access information. *For example, information relating to the release of the file under the Human Rights Convention, or intellectual property restrictions.*	0-n	8.1.29
12.4.22	Keyword-based name.	0-n	3.2.6
12.4.23	Other name.	0-1	3.2.7
12.4.24	Descriptive terms.	0-n	3.2.8

12.5 Metadata Elements for File or File Volume

Some metadata elements can validly be held against either files or against their volumes. This is because of the varying ways file volumes can be used, as explained in section 2.2 under the heading "Electronic File and Volume".

Users of this specification therefore must determine the correct level for these metadata elements according to their needs. For example management decisions on security classification, disposal and review can be taken at the file or volume level. In some ERMS implementations, all these may be at the file level; in others they may all be at the volume level; and in yet others it may depend on the file.

The ERMS must support the following for each file or file volume:

Ref.	Metadata element	Occurs	Req.
12.5.1	Retention schedule (or, if requirement 5.1.5 is not supported, disposal review date or event and disposal instructions).	1-n	5.1.4 5.1.5 10.2.1
12.5.2	Date opened.	1	3.3.2
12.5.3	Date closed.	0-1	3.4.9
12.5.4	Where export to some other organisation(s) (e.g. state or national archives) is envisaged, identifier of the organisations to which the file is to be exported.	0-n	5.3.1 5.3.17
12.5.5	Status of transfer.	0-n	5.3.7
12.5.6	Physical/hybrid indicator.	1	10.1.1 10.1.2 10.1.3 10.2.4
12.5.7	Physical location (for physical files).	1	4.4.2 10.1.4
12.5.8	Check-out/check-in status (for physical files).	1	4.4.2 10.1.5 10.2.8
12.5.9	Date checked out (for physical files).	1	4.4.2 10.2.8
12.5.10	Checked out to (for physical files).	1	4.4.2 10.2.8
12.5.11	Bring forward date (for physical files).	1-n	10.2.9
12.5.12	Bring forward to (for physical files).	1-n	10.2.9
12.5.13	Bring forward text (for physical files).	1-n	10.2.9
12.5.14	Destruction Status.	1	5.1.4 5.3.17

Ref.	Metadata element	Occurs	Req.
12.5.15	Destruction date and user.	0-1	9.3.7
12.5.16	Review comment.	0-n	5.2.6
12.5.17	Date destroyed.	0-1	5.3.15
12.5.18	User-defined metadata elements.	0-n	N/A

The ERMS should support the following for each file or file volume:

Ref.	Metadata element	Occurs	Req.
12.5.19	If requirement 12.4.10 is supported, date on which security classification should be reviewed.	0-1	4.6.12
12.5.20	Barcode and/or other physical location data (for physical files).	0-1	10.1.9
12.5.21	Logical deletion or move of file.	0-1	9.3.1
12.5.22	Transfer, move or deletion status of hybrid file.	0-n	5.3.9

12.6 Volume Metadata Elements

The ERMS must support the following for each volume:

Ref.	Metadata element	Occurs	Req.
12.6.1	Identifier.	1	3.3.1 7.1.1
12.6.2	Physical/hybrid indicator.	0-1	10.1.1 10.1.2 10.1.3
12.6.3	User-defined metadata elements.	0-n	N/A

12.7 Record Metadata Elements

The ERMS must support the following for each record:

Ref.	Metadata element	Occurs	Req.
12.7.1	Identifier.	1	7.1.1
12.7.2	Subject.	1	6.1.2 10.3.5

Ref.	Metadata element	Occurs	Req.
12.7.3	Author. *May be an individual or organisation. To be captured automatically whenever possible.*	1	6.1.2 6.4.3 10.3.5
12.7.4	Person or post responsible for maintenance of the record in the ERMS.	0-1	4.1.7
12.7.5	Date (and time if appropriate) of compilation of the record. *For example:* • *where the record is a letter, the date at the top of the letter;* • *where the record is a sound or other recording of a period in time, the start and end times.* *To be captured automatically whenever possible.*	1	6.1.2 10.3.5
12.7.6	Addressee(s). *Individual(s) and/or organisation(s) to which the information in the record was addressed. To be captured automatically whenever possible.*	1-n	6.1.2 6.4.3
12.7.7	Record type. *Typically letter, invoice, memorandum etc. To be captured automatically whenever possible.*	1	6.1.2 10.3.5
12.7.8	Registration date/time. *To be captured automatically.*	1	6.1.7
12.7.9	User group access rights. *Information about which user groups can access the record, and the kinds of access they are allowed.*	0-n	4.1.1
12.7.10	User access rights. *Information about which users can access the record, and the kinds of access they are allowed.*	0-n	4.1.1
12.7.11	Security category. *To be captured automatically from the document forming the record whenever possible.*	0-1	4.6.1

Ref.	Metadata element	Occurs	Req.
12.7.12	Security category history, i.e. for each previous classification: • category; • dates of change; • reason for change; • user responsible for change.	0-n	9.3.6
12.7.13	Preservation metadata (where the ERMS is expected to preserve the record for longer than the anticipated life cycle of the source applications). This typically includes but need not be limited to: • file names; • hardware dependencies; • operating system dependencies; • application software dependencies (application names and versions); • file formats; • resolution; • compression algorithm version and parameters; • encoding scheme; • rendition information. *May be multiple values where compound documents are included.*	1-n	6.1.2 8.2 8.3 8.4 11.7.7
12.7.14	Vital record indicator.	1	4.3.6
12.7.15	Extract identifier(s).	0-n	8.1.26
12.7.16	Retention schedule.	0-n	5.1.4 5.1.5
12.7.17	Status of transfer.	0-n	5.3.17
12.7.18	User-defined metadata elements.	0-n	N/A

The ERMS should support the following for each electronic record:

Ref.	Metadata element	Occurs	Req.
12.7.19	Date at which security classification is to be reviewed.	0-1	4.6.12

Ref.	Metadata element	Occurs	Req.
12.7.20	Electronic signature(s), certificate(s), counter-signature(s).	0-n	10.5.7
12.7.21	Electronic signature authentication(s), including certification authority, date and time checked.	0-n	10.5.1 10.5.4
12.7.22	Date sent. *To be captured automatically whenever possible.*	1	6.1.2
12.7.23	Date received. *To be captured automatically whenever possible.*	1	6.1.2
12.7.24	Links to related records.	0-n	11.1.18
12.7.25	Intellectual property restrictions. *For example, rules about use of the information in the record and copyright payments due.*	0-n	8.1.29
12.7.26	Document version.	0-n	6.1.10
12.7.27	Language.	0-n	11.4.11
12.7.28	Encryption information.	0-1	10.6.2
12.7.29	Electronic watermark information.	0-1	10.7.1

12.8 Record Extract Metadata Elements

The ERMS must support the following for each record extract:

Ref.	Metadata element	Occurs	Req.
12.8.1	Identifier.	1	7.1.1 9.3.11
12.8.2	Identifier of original record.	1	8.1.26
12.8.3	Extract creation date.	1	9.3.11
12.8.4	Identifier of user who created extract.	1	9.3.11
12.8.5	Reason for creation.	0-1	9.3.11
12.8.6	User-defined metadata elements.	0-n	N/A

12.9 User Metadata Elements

The ERMS must support the following for each user:

Ref.	Metadata element	Occurs	Req.
12.9.1	User identifier.	1	4.1.1

Ref.	Metadata element	Occurs	Req.
12.9.2	User role.	1-n	4.1.3
12.9.3	User group membership.	0-n	4.1.5
12.9.4	User access rights.	0-n	4.1.1
12.9.5	Expiry date for access rights.	1	4.1.2
12.9.6	User security clearance (where required by the environment).	1	4.6.7
12.9.7	Expiry date for clearance.	1	4.6.12
12.9.8	User-defined metadata elements.	0-n	N/A

12.10 Role Metadata Elements

The ERMS must support the following for each role:

Ref.	Metadata element	Occurs	Req.
12.10.1	Role name.	1	4.1.3
12.10.2	Role group membership.	0-n	4.1.3
12.10.3	Role access rights.	0-n	4.1.1
12.10.4	Expiry date for access rights.	1	4.1.2
12.10.5	Role security clearance (where required by the environment).	1	4.1.3
12.10.6	Expiry date for clearance.	1	4.6.12
12.10.7	User-defined metadata elements.	0-n	N/A

12.11 Customisation Notes for Metadata Requirements

Users of this specification should analyse their application's requirements for metadata and amend the above accordingly.

After identifying which metadata elements are needed, they should identify for each element the following attributes:

- field format (see 12.1.5) and length;
- obligation (mandatory or optional);
- source of data (see 12.1.9, 12.1.10, 12.1.11, 12.1.12);
- nature of validation (see 12.1.13, 12.1.14, 12.1.15);
- inheritance rules (see 12.1.11);

- default value rules for data entry (e.g. declaration date may default to current date, whereas record type may have to be entered manually).

It will only be possible to specify requirements in detail once this has been achieved.

Note that the validation, automatic capture, inheritance and default value rules are especially important for usability and acceptably low error rates where the system is to be used in an ongoing office operation (as opposed to in a dedicated archive).

13 REFERENCE MODEL

13.1 Glossary

This glossary defines key terms used in the MoReq Specification (i.e. in the requirements as well as in this model).

Some significant definitions are taken from, or closely adapted from, glossaries presented in reference publications listed in Annex 1; these sources are acknowledged below each definition.

Terms defined within this glossary are shown in *italics*.

Administrator

A role responsible for the day to day operation of the corporate records management policy within the organisation.

This represents a simplification. Especially in large organisations, the tasks attributed in this specification to Administrators may be divided between several roles, with titles such as Records Manager, Records Officer, Archivist etc.

audit trail

Information about transactions or other activities which have affected or changed entities (e.g. metadata elements), held in sufficient detail to allow the reconstruction of a previous activity.

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 (usually for manual activities); but the former are the focus of this specification.

authenticity

(in the context of records management only) The quality of being genuine.

Source: Adapted and abbreviated from the definition of "record authenticity" in the UBC-MAS Glossary (Annex 1 reference [8]).

Note: in the context of a *record*, this quality implies that a record is what it purports to be; it does not address the trustworthiness of the record's content as a statement of fact.

Note: authenticity is conferred on a record by its mode, form, and/or state of transmission, and/or manner of preservation and custody. For further details refer to the UBC-MAS Glossary (as above).

capture

Registration, *classification*, addition of *metadata* and storage of a *record* in a system that manages *records*.

class

(in this specification only) The portion of a hierarchy represented by a line running from any point in the classification scheme hierarchy to all the files below it.

Note: this can correspond, in classical terminology, to a “primary class”, “group” or “series” (or sub-class, sub-group, sub-series etc.) at any level in the classification scheme.

classification (verb)

Systematic identification and arrangement of business activities and/or *records* into categories according to logically structured conventions, methods, and procedural rules represented in a classification scheme.

Source: ISO 15489 (draft international standard; see Annex 1 reference [9]).

classification scheme

See classification.

Source: definition of “Classification System” in ISO 15489 (draft international standard; see Annex 1 reference [9]).

Note: a classification scheme is often represented as a hierarchy.

clearance

See security clearance.

close (verb)

The process of changing the attributes of an *electronic file volume* so that it is no longer able to accept the addition of *records*.

closed

Describes an *electronic file volume* which has been closed and so cannot accept the addition of *records*.

configuration time

The point in the lifecycle of the ERMS at which it is installed and its parameters are established.

destruction

Process of eliminating or deleting records, beyond any possible reconstruction.

Source: ISO 15489 (draft international standard; see Annex 1 reference [9]).

digital

See *electronic.*

document (noun)

Recorded information or object which can be treated as a unit.

Source: ISO 15489 (draft international standard; see Annex 1 reference [9]).

Note: a document may be on paper, microform, magnetic or any 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 objects.

Note: documents differ from *records* in several important respects.

EDMS

Electronic Document Management System.

Note: the functionality required for EDMS is not included in this specification. However, an EDMS is often used in tight integration with an *ERMS*. See section 10.3 for more details.

electronic

For the purposes of this specification, the word "electronic" is used to mean the same as "digital".

Note: analogue recordings, though they may be regarded as electronic, are not considered as "electronic" for the purposes of this specification as they cannot be stored within a computer system unless they are converted to digital form. It follows that, in the terminology of this specification, analogue records can only be stored as *physical records.*

electronic document

A *document* which is in electronic form.

Note: use of the term *electronic document* is not limited to the text-based documents typically generated by word processors. It also includes e-mail messages, spreadsheets, graphics and images, HTML/XML documents, multimedia and compound documents, and other types of office document.

electronic file

A set of related *electronic records*.

Source: PRO Functional Specification of "electronic file" (Annex 1 reference [2]).

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

electronic record

A *record* which is in *electronic* form.

Note: it can be in electronic form as a result of having been created by application software or as a result of digitisation, e.g. by scanning paper or microform.

ERMS

Electronic Record Management System.

Note: ERMS differ from *EDMS* in several important respects. See section 10.3 for more details.

export (noun)

The process of producing a copy of complete *electronic files* for another system.

Note: the files remain on the ERMS after export, unlike *transfer*.

extract

(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.

Source: definition of "instance" in PRO Functional Specification (Annex 1 reference [2]).

Note: the changes usually result from restrictions on disclosure of information. For example, a *record* may be made available only after individuals' names are masked or removed from it; in this case, an *extract* of the record is created in which the names have been made illegible. The process of masking is sometimes referred to as redaction.

file (noun)

(1) Where this term is used in isolation, it refers to both *electronic files* and *paper files*.

(2) When used with qualification, i.e. *electronic file* or *paper file*, the relevant definition applies.

hybrid file

A set of related *electronic records* and/or *physical records* stored partly in an *electronic file* within the *ERMS* and partly in a related *paper file* outside the *ERMS*.

Source: definition of "hybrid file" in PRO Functional Specification (Annex 1 reference [2]).

metadata

(in the context of records management) Structured or semi-structured information which enables the creation, management and use of records through time and within and across domains in which they are created.

Source: Archiving Metadata Forum working definition (http://www.archiefschool.nl/amf).

Note: the distinction between data and its metadata can be unclear. For example, it is usually clear that the essential indexing data for a record (title, date etc.) is part of that record's metadata. However, the audit trail for a record, or the retention schedule for a record, can validly be considered to be either data or metadata, depending on the context. Different types of metadata can be defined, for example, for indexing, for preservation, for rendering etc. These details of metadata usage are beyond the scope of the MoReq specification.

open

(verb) The process of creating a new *electronic file volume*.

(adjective) Describes an *electronic file volume* which has not yet been *closed*, and so is able to accept the addition of *records*.

paper file

A device for holding *physical documents*.

Source: PRO Functional Specification (Annex 1 reference [2]).

Note: examples of paper files include, among others, envelopes, box files and ring binders.

PDF

Portable Document Format.

Note: this format is proprietary to Adobe Inc., but is widely used. Its inclusion in this glossary does not represent any form of endorsement.

record (noun)

Document(s) produced or received by a person or organisation in the course of business, and retained by that person or organisation.

Source: adapted from PRO Functional Specification (Annex 1 reference [2]).

Note: Local national definitions may also apply.

Note: a record may incorporate one or several *documents* (e.g. when one document has attachments), and may be on any medium in any format. In addition to the content of the document(s), it should include contextual information and, if applicable, structural information (i.e. information which describes the components of the record). A key feature of a record is that it cannot be changed.

redaction

The process of hiding sensitive information in a *record*.

Note: this can include applying opaque rectangles to obscure names etc. (the electronic equivalent of censoring paper documents with ink) or removing individual pages.

Note: in all cases the totality of the original *electronic record* is not affected. Redaction is carried out on a copy of the electronic record; this copy is called an *extract*.

registration

The act of giving a *record* a unique identifier on its entry into a system.

Source: ISO 15489 (draft international standard; see Annex 1 reference [9]).

Note: registration usually implies the recording into a "register" of important metadata, e.g. "all the data necessary to identify the persons and acts involved and the documentary context of the records" (UBC-MAS Glossary, Annex 1 reference [x]).

render

The process of producing a *rendition*.

rendition

The manifestation of an *electronic record* presented (i.e. rendered) to which a *user* can refer.

Note: this may include on-screen display, printed and audio and multimedia presentations.

Note: the exact nature of the rendition can be affected by the software and hardware environment. Typically different renditions of the same *record* can vary in details of font metrics, line endings and pagination, resolution, bit depth, colour space etc. In most cases these differences are acceptable. However, in some cases their potential effects have to be considered separately; these considerations are beyond the scope of this specification.

repertory

A list of existing file titles within each of the lowest levels of the classification scheme.

retention schedule

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

Source: adapted from definition of "disposal schedule" in PRO Functional Specification (Annex 1 reference [2]).

role

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

Source: PRO Functional Specification (Annex 1 reference [2]).

security category

One or several terms associated with a *record* which define rules governing access to it.

Note: security categories are usually assigned at an organisational or national level. Examples of security categories used in government organisations throughout most of Europe are: "Top Secret", "Secret", "Confidential", "Restricted", "Unclassified". These are sometimes supplemented by other terms such as "WEU Eyes Only" or "Personnel".

Note: this term is not in general use.

security clearance

One or several terms associated with a *user* which define the *security categories* to which the *user* is granted access.

SQL

Structured Query Language.

Note: this defines a standard for relational databases, which are commonly used to store ERMS metadata. The standard is defined in ISO 9075 (see Annex 7).

transfer (verb)

The process of moving complete *electronic files* to another system.

Source: adapted from PRO Functional Specification (Annex 1 reference [2]).

Note: the files are often transferred together with all other files in a *class* of the *classification scheme* when the purpose of transfer is to move the files to an archive for permanent preservation.

Note: see also *export*.

user

Any person utilising the *ERMS*.

Note: this may include (among others) Administrators, office staff, members of the general public, and external personnel such as auditors.

version

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

Source: PRO Functional Specification (Annex 1 reference [2]).

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; see also *extract*.

volume

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

Source: Definition of "part" in PRO Functional Specification (Annex 1 reference [2]).

Note: the subdivisions are created to improve manageability of the file contents by creating units which are not too large to manage successfully. The subdivisions are mechanical (e.g. based on number of records or ranges of numbers or time spans) rather than intellectual.

13.2 Entity-Relationship Model

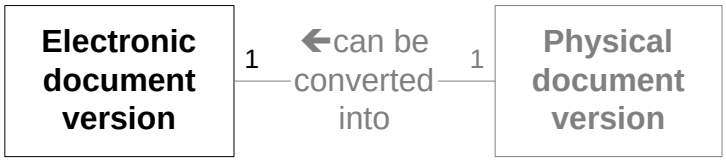
This section repeats section 2.3, for ease of reference.

It contains an entity-relationship model which can be used as an aid to understanding the specification. Section 13.3 contains a narrative explanation.

An important aspect of this diagram is that it does not represent actual structures stored in the ERMS. It represents a view of the metadata associated with records. An ERMS uses this metadata to produce behaviour equivalent to the structures in the diagram. See section 2.2 for further explanation of this point.

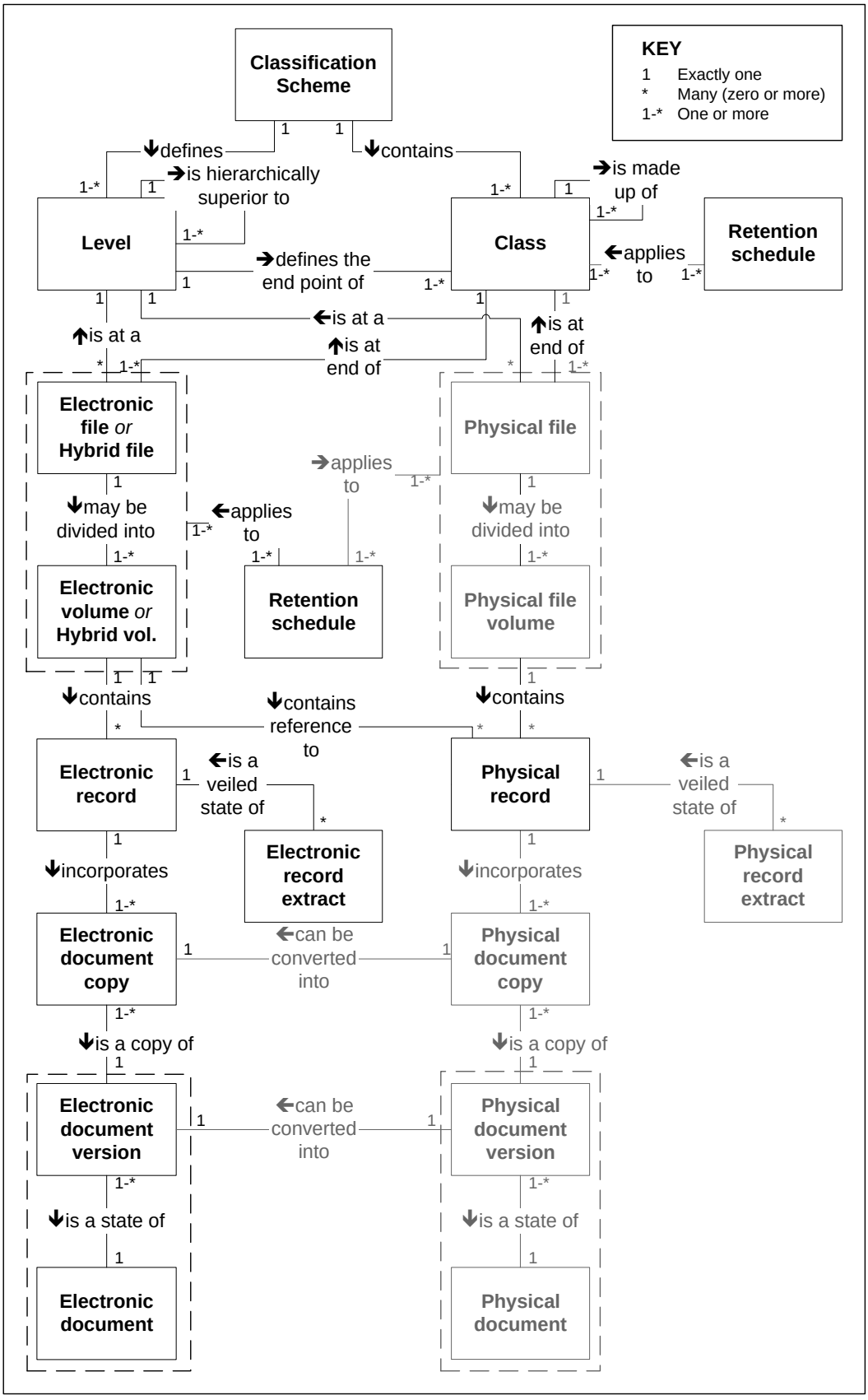
The relationships between files, volumes, records and other important entities are depicted more rigorously in the following entity-relationship diagram. This is a formal representation of selected structures which comprise an ERMS.

In the diagram, entities – files, records and so on – are represented by rectangles. The lines connecting them represent the relationships between the entities. Each relationship is described by text in the middle of the line; and this should be read in the direction of the arrow. Each end of the relationship has a number which represents the number of occurrences (strictly, the cardinality); the numbers are explained in the key. So, for example, the following extract:



means "One physical document version can be converted into one electronic document version" (note the direction of the relationship arrow).

Note that the entity Class is related to itself by the relationship "is made up of". This recursive relationship describes, in formal terms, the hierarchy of folders, in which a Class may contain other Class. Similarly, each Level may be hierarchically superior to other Levels.


Classification Scheme
KEY
1 Exactly one
* Many (zero or more)
1-* One or more
defines
contains
is hierarchically superior to
is made up of
Level
Class
Retention schedule
defines the end point of
applies to
is at a
is at end of
Electronic file or Hybrid file
Physical file
may be divided into
applies to
Electronic volume or Hybrid vol.
Retention schedule
Physical file volume
contains
contains reference to
Electronic record
Physical record
is a veiled state of
Electronic record extract
Physical record extract
incorporates
Electronic document copy
can be converted into
Physical document copy
is a copy of
Electronic document version
Physical document version
is a state of
Electronic document
Physical document

13.3 Entity-Relationship Diagram Narrative

The entity-relationship diagram in section 13.2 shows a wider context in which electronic records exist. For clarity, it includes more detail about the relationship between paper and electronic records and documents than other chapters in this specification.

This specification does not focus strongly on the management of physical records; they are dealt with only enough to relate some continuing paper records to electronic records in the ERMS. Accordingly, most of the paper entities and relationships are shown in grey rather than the black used for their electronic counterparts.

Note that the diagram is a simplified model; it does not attempt to represent all possible entities or relationships. Rather, it shows only the most significant ones for this application. For example, it does not show users, roles etc.

The remainder of this narrative describes the entities in the diagram, and their inter-relationships.

Classification Scheme

In order to practice records management principles, an organisation must have at least one classification scheme. This sets out the filing structure (typically consisting of hierarchy, numbers, names and descriptions) for a defined part of the organisation.

Level

The classification scheme is generally represented as a hierarchy, or tree structure. The hierarchy includes a number of levels, corresponding to the "tops" of classes, groups, sub-classes etc. used to describe classification schemes for physical systems. Each level may have further levels "beneath" it in the hierarchy.

Class

The classification scheme can be viewed as a hierarchy made up of a number of classes, much as a tree is made up of branches. Each class is connected to the hierarchy at one level; can extend over several levels; and can contain smaller classes. Several classes can start at any single level; but each class starts only at one level.

File

Files occur at the end of classes, at any level in the hierarchy, much as leaves are found at the ends of tree branches. Each is either an electronic file, a physical file

or a hybrid file. A physical file is the conventional container used to store physical documents and/or records (i.e. paper, audiotape, etc. rather than electronic).

Volume

Files can be divided into volumes, according to specific rules. In practice, some files are not divided into volumes. The rules may depend on size or number of records, or may depend on transactions or time periods. This practice originated with physical files, in order to restrict them to a manageable size and weight. The practice is, where appropriate, continued with electronic files, to limit them to a manageable length for review, transfer, etc.

The terms file and volume are, in practice, sometimes used loosely or interchangeably. For example, a user will typically ask for "a file" rather than (more accurately) asking for "a volume." This is especially apparent when a physical file consists only of one volume; in this case, although the file analytically is made up of one volume, it is not always labelled as a volume (often, the label is only applied when the second volume is opened). Strictly, all end users interact with volumes, but this is often simplified to files. A pecked box has been drawn around electronic file and electronic volume (and around the corresponding physical entities). This is to reflect the reality that using the term electronic volume instead of electronic file could hinder understanding.

Retention Schedule

Two rectangles in the figure represent retention schedules. This is solely for ease of layout in the diagram; the two rectangles represent a single entity.

A retention schedule specifies the rules for keeping and disposing of records. The ERMS can contain several schedules, one or more of which are applied to each class, file or volume.

Record

At the heart of the system lies the most important entity, the records. These are the reason for the entire records management infrastructure, as they form the account 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. Records are organised into files, with several records per file.

Record extract

It is sometime necessary to produce a sanitised (i.e. censored) copy of a record, for example to remove sensitive personal names. As records cannot themselves by modified, this is referred to as producing a record extract. The process of

producing a record extract consists of taking a copy of the record (leaving the original unchanged) and sanitising the copy.

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. They frequently 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. They may also be in the form of image files obtained by scanning paper documents.

Documents can exist in several document versions. As with file and volume, 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, this document uses the term electronic document loosely, to mean electronic document version in most cases.

A physical document copy can be converted into an electronic record copy, by scanning or other means of digitisation. Several physical document copies can also be converted into a single electronic record copy, for example a cover note attached to a report. Contrarily, one physical document copy can be converted into several electronic record copy, for example one invoice could be converted into an electronic record in electronic files for both supplier and a product.

13.4 Access Control Model

This section contains a simple generic model of user roles. In order to make it generic, it consists of a matrix which recognises just two user roles. The roles – user, and Administrator – are defined in terms of access to ERMS functionality.

The role Administrator represents a simplification. Especially in large organisations, the tasks attributed in this specification to Administrators may be divided between several roles, with titles such as Administrator, Records Manager, Records Officer, Archivist and Data Manager or IT manager etc.

Note that the Administrator role is in many cases only implementing, from a system perspective, decisions taken by more senior management based on laws and regulations, such as information laws, data security laws, archival laws and industry regulations; see section 11.5. This matrix is not intended to imply that Administrators must take management decisions, though in some environments that may be the case.

In broad terms, users have access to facilities which an office worker or researcher needs when using records. This includes adding documents, searching for and retrieving records; their interest is in the contents of records. Administrators take actions related to the management of records themselves; their interest is in records as entities rather than their content. They also manage the ERMS hardware, software and storage, ensuring backups are taken and the performance of the ERMS.

In the following table,

- YES indicates the ERMS must allow this combination of roles and functions;
- NO indicates the ERMS must prevent this combination of roles and functions;
- OPTIONAL indicates that the ERMS may allow or prevent this combination of roles and functions, and that the using organisation must determine whether its procedures allow or prevent this combination.

Note that this matrix is divided into sections. These sections group, for convenience, the functions normally associated with files, records, records management and administration.

This matrix is best viewed as a starting point, and as the formal basis for assigning rights. Users of this specification will need to consider additional requirements which are specific to their environment. For example, some environments may have “records reviewer” roles which are separate from the Administrator roles; in this case there will be a need to specify access controls for this role.

Access Matrix

Function	User role	
	User	**Administrator**
Create new files	OPTIONAL	YES
Maintain classification scheme and files	NO	YES
Delete files	NO	YES
Capture records	YES	YES
Search for and read records	YES[2]	YES[2]
Change content of records	NO	NO[3]
Change record metadata	NO	YES
Delete records	NO	YES
Retention schedule & disposal transactions	NO	YES
Export and import files and records	NO	YES
View audit trails	OPTIONAL	YES
Change audit trail data	NO	NO
Move audit trail data to off-line storage media	NO	YES
Perform all transactions related to users and their access privileges	NO	YES
Maintain database and storage	NO	YES
Maintain other system parameters	NO	YES
Define and view other system reports	NO	YES

[2] Subject to access rights for individual documents.

[3] Except for redaction – see section 9.3.

ANNEXES

Annex 1 - Reference Publications

This specification was prepared with reference to the following existing specifications and reference models.

Ref.	Name and Ownership or Source	URL or Publication Details
[1]	Dublin Core Metadata Element Set, Version 1.1: Reference Description	http://purl.oclc.org/dc/documents/rec-dces-19990702.htm or http://mirrored.ukoln.ac.uk/dc/
[2]	Functional Requirements for Electronic Records Management Systems (GB Public Record Office)	http://www.pro.gov.uk/recordsmanagement/eros/invest/default.htm
[3]	Functional Requirements for Evidence in Record Keeping (US University of Pittsburgh)	http://www.lis.pitt.edu/~nhprc/
[4]	Guide for Managing Electronic Records from an Archival Perspective (Committee on Electronic Records, International Committee On Archives, ICA Study 8)	http://data1.archives.ca/ica/cer/guide_0.html
[5]	Code of Practice for legal admissibility and evidential weight of information stored electronically (British Standards Institution)	Published by British Standards Institution (www.bsi-global.com) as BSI DISC PD 0008
[6]	Guidelines on best practices for using electronic information (DLM Forum)	http://europa.eu.int/ISPO/dlm/documents/guidelines.html
[7]	ISAD(G): General International Standard Archival Description, Second Edition (Committee on Descriptive Standards, International Council on Archives)	http://www.ica.org/cgi-bin/ica.pl?04_e
[8]	The Preservation of the Integrity of Electronic Records (UBC-MAS Project)(University of British Columbia)	http://www.slais.ubc.ca/users/duranti/
[9]	Records Management, ISO 15489 (International Organization for Standardization)	To be published by the International Organization for Standardization; the standard was at the stage of a draft international standard at the time of writing.
[10]	Records/Document/Information Management: Integrated Document Management System for the Government of Canada - Request for Proposal - Requirements (RDIM)(National Archives of Canada)	originally published in 1996 ar http://www.archives.ca/06/4rdims.pdf; may now be unavailable, see also http://www.rdims.gc.ca/
[11]	Standard 5015.2 “Design Criteria Standard For Electronic Records Management Software Applications” (US Department of Defense)	http://jitc.fhu.disa.mil/recmgt/

Annex 2 - Development of this Specification

The MoReq specification was developed for the European Commission by Cornwell Affiliates plc, a consultancy firm based in the United Kingdom. The project team included specialist consultants, who authored the specification, and a group of records management experts from several countries; see Annex 4 part 1 for details of authors and contributors.

A project initiation meeting was held in London, involving the entire team. At this meeting, working protocols and other principles were agreed, and, some key references were identified. This was the only full meeting of the team; the remainder of the project was managed almost entirely using e-mail.

The next step involved desk research, searching for and obtaining copies of relevant reference works. The references were examined by the consultants, leading to a list of references used, which is at Annex 1.

The next step was to analyse the selected references for structure and content. These were compared, and a structure was drafted which could be mapped onto the tables of contents of the references.

The consultants then started to draft the specification, using the draft structure as a basis. They went through the references, line by line in almost all cases, ensuring that every requirement – implicit or explicit – was included in MoReq. During this drafting, the structure evolved slightly, as more logical groupings of requirements became apparent; this evolution continued throughout the project.

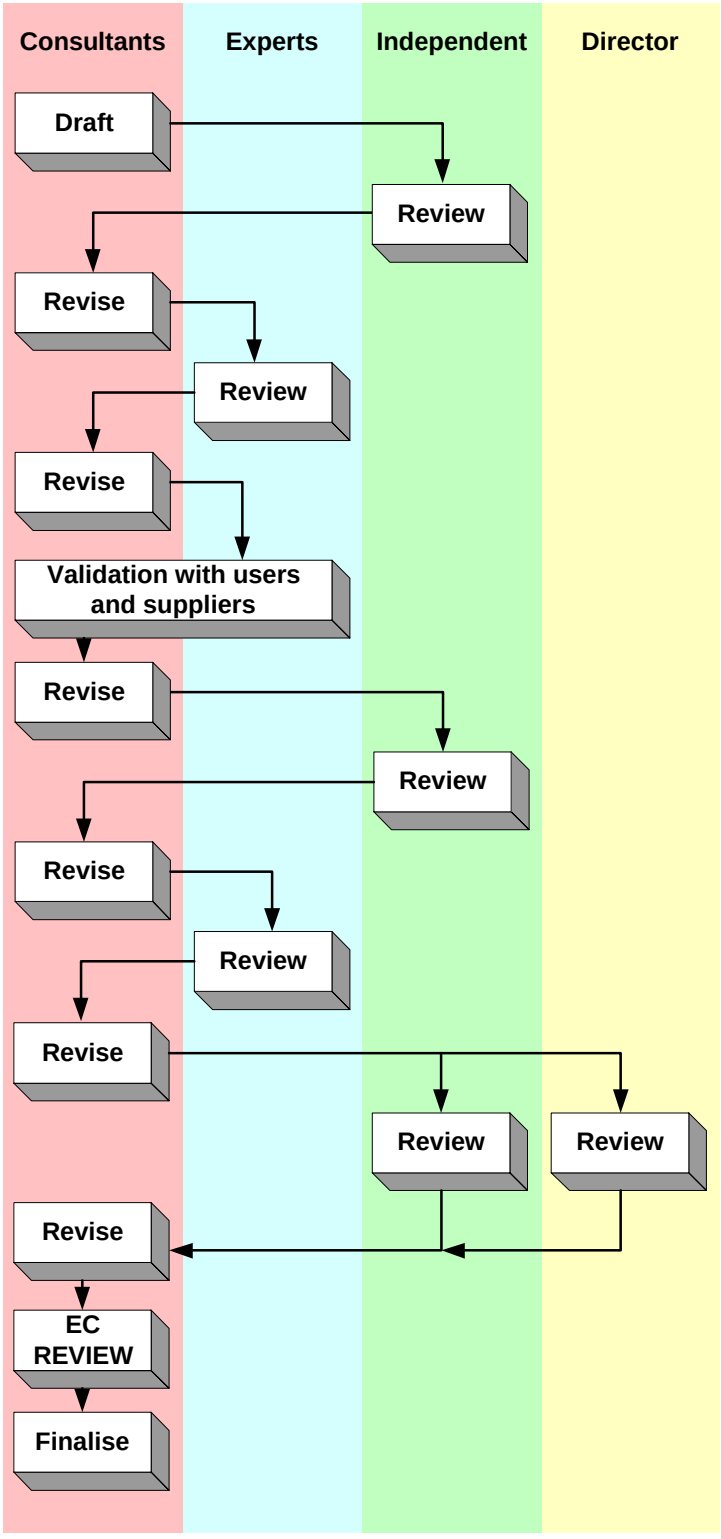
The first draft was then submitted to the first of several reviews, as the beginning of a traditional review/revise iterative development. The iterative reviews included five different kinds of review:

- cross-reviews by the consultants of each other's work;
- reviews by a semi-independent records management expert, who was not involved in any of the discussion development. He was charged especially with reconciling the early drafts with the reference publications;
- reviews by a group of international experts;
- reviews by the European Commission Project Officer;
- quality assurance checks by the Cornwell Affiliates plc Project Director.

During this iterative process, the consultants and the experts exchanged ideas, comments and other points.

When the specification was almost complete, it entered a formal validation exercise. A questionnaire was developed. This, with the draft specification, was sent to ERMS suppliers and Records Managers from a variety of organisations who had kindly agreed to participate (see Annex 4 part 2). They reviewed the product for fit with existing products and for usability in the context of their organisation.

The process is shown diagrammatically in the following deployment flowchart.



Annex 3 - Use of this Specification in Electronic Form

This specification has been prepared so that it can be used in electronic form. It has been prepared using Microsoft® Word 97.

The main advantage of using the specification in electronic form is that it can easily be customised.

All cross references are hyperlinks which can be used for navigation by a single click. For example, in the phrase "see the Glossary in section 13.1" both the section number and section name are hyperlinks.

The requirements are presented in the form of tables, with one requirement per table row. This is illustrated below.

The tables consist of three columns:

- **number:** a requirement reference number. This is generated automatically by Microsoft Word, as the numbers use a "heading" style. The result is that if chapters, sections or requirements are added or subtracted, the numbering changes automatically;
- **requirement:** the requirement text. This always uses one of the verbs "must" (to indicate a mandatory requirement) or "should" (to indicate a desirable requirement);
- **spare column:** this can be used for scoring responses if the specification is used for tendering, for adding weightings, or other information. It can be widened, narrowed, or deleted. It uses the Microsoft Word style "Mand/Des".

Note that if chapters, sections or requirements are deleted, Microsoft Word will replace any cross-references to them (if there are any) with an error message. These can be located by searching for the text "**error!**" This is especially relevant to chapter 12 (Metadata Requirements), which contains many cross-references.

By default, the table borders are not visible. They can be seen by use of the "Show Gridlines" command.

Chapter 12 uses a variation of the table shown above; it introduces an additional column which cross-refers to requirement statements. These cross-references are hyperlinks to the requirements.

Annex 4 - Acknowledgements

1 Project Team

This specification was authored by:

- Marc Fresko
- Martin Waldron

with expert review and additional input provided by:

- Francisco Barbedo, Porto State Archive (Portugal)
- Keith Batchelor, independent consultant (United Kingdom)
- Nils Brübach, Archives School, Marburg (Germany)
- Miguel Camacho, SADIEL S.A. (Spain)
- Luciana Duranti, School of Library and Information Studies, University of British Columbia (Canada)
- Mariella Guercio, University of Urbino, Institute for Archival and Librarian Studies (Italy)
- Peter Horsman, Netherlands Institute for Archival Education and Research (The Netherlands)
- Jean-Pierre Teil, National Archives (France)

The Project Director was Keith Cornwell, Managing Director of Cornwell Affiliates plc, and the European Commission Project Officer was Paul E. Murphy, IDA Programme, DG Enterprise.

Thanks are due to Sue Wallis, Jane Burnand and Neil Grosse of Cornwell Affiliates plc for providing administrative support.

2 Validation Organisations

The project team is grateful to the following organisations which kindly participated in the validation exercise:

Company	**Type of Organisation**	**Country**
Pfizer	Pharmaceutical Manufacturer	UK
DERA	Defence Agency	UK
HM Treasury	Central Government	UK
Tower Technology	ERMS Supplier	UK
Technostock	Consultancy	Spain
Ministry of Justice	Central Government	Italy

3 Trademarks

All trademarks appearing in this specification are acknowledged. Proprietary products are mentioned for illustrative purposes only; their inclusion does not represent any form of endorsement. Similarly, exclusion of other products implies no criticism of these products.

Annex 5 - Correspondence to Other Models

1 Correspondence to Dublin Core Metadata Model

The metadata elements described in chapter 12 can be mapped to the Dublin Core Metadata Element Set (see Annex 1 ref. [1]). A possible mapping is shown, for information, in the following table.

	MoReq	
Dublin Core Element Name	**Requirement Numbers**	**Element Description**
Title	12.7.1	Identifier
Creator	12.7.3	Author
Subject	12.4.2 12.4.3 12.4.22 12.7.2	Name Descriptive keyword refs. Keyword-based name Subject
Description	12.4.4	Description
Publisher	-	none
Contributor	-	none
Date	12.7.5 12.7.8 12.7.22 12.7.23	Date/time Registration date/time Date sent Date received
Type	12.7.7	Record type
Format	12.7.13	Preservation metadata
Identifier	12.7.1	Unique identifier
Source	12.8.2	Identifier of original record (extracts only)
Language	-	none
Relation	12.7.24	Links to related records
Coverage	-	none
Rights	12.7.25	Intellectual property restrictions

2 Correspondence to Pittsburgh metadata model

The metadata elements described in chapter 12 can be mapped to the "Pittsburgh Metadata Model" (see Annex 1 ref. [9]). A possible mapping is shown, for information, in the following table. However, the mapping is not straightforward, due to the differences in paradigm and emphasis between MoReq and the Pittsburgh study. Consequently some of the mappings may be subject to interpretation.

	MoReq	
Pittsburgh Model Description	**Requirement Numbers**	**Element Description**
Handle layer		
Registration	12.7.1 12.7.8	Identifier Date/time
Record Identifier	12.7.1	Identifier
Info. discovery & retrieval	12.4.2 12.4.3 12.4.22 12.7.2	Name Keyword references Keywords Subject
Terms and conditions layer		
Rights status	12.4.8 12.4.9 12.4.10 12.7.9 12.7.10 12.7.11	User group access rights User access rights Security category User group access rights User access rights Security category
Access	12.7.25 12.4.21	Intellectual property restrict'ns Other access information
Use	-	none
Retention	12.4.17 12.5.1	Retention schedule Retention schedule

	MoReq	
Pittsburgh Model Description	**Requirement Numbers**	**Element Description**
Structural layer		
File identification	-	none
File encoding	12.7.20 12.7.21 12.7.28 12.7.29	Electronic signatures (etc.) Electronic signature authenticns. Encryption information Watermark information.
File rendering	12.7.13	Preservation metadata
Record rendering	12.7.13	Preservation metadata
Content structure	-	none
Source	12.7.27	Language

Annex 6 - Date Processing

The ERMS is required to process all dates correctly, regardless of millennium, century or other date representation issues – see 11.5.1. This annex presents a statement of the requirement for year 2000 processing which could be adapted, if necessary, to deal with other dates. This will be especially relevant for Electronic Records Management Systems which may include metadata dates for previous or future centuries.

The following is reproduced verbatim, with permission, from BSI DISC PD2000-1:1998 A Definition of Year 2000 Conformity Requirements (see Annex 7 section 2).

Year 2000 conformity shall mean that neither performance nor functionality is affected by dates prior to, during and after the year 2000.

In particular:

Rule 1 No value for current date will cause any interruption in operation.

Rule 2 Date-based functionality must behave consistently for dates prior to, during and after year 2000.

Rule 3 In all interfaces and data storage, the century in any date must be specified either explicitly or by unambiguous algorithms or inferencing rules.

Rule 4 Year 2000 must be recognized as a leap year.

Annex 7 – Standards and Other Guidelines

This annex lists standards and other resources referenced in the specification.

1 Standards

BS 4783
: Storage, transportation and maintenance of media for use in data processing and information storage (in several parts)

BS 7978
: Bundles for the Perpetual Preservation of electronic documents and associated objects

ISO 639
: Codes for the representation of names of languages

ISO 3166
: Codes for the representation of names of countries

ISO 8601
: Data elements and interchange formats – Information interchange – Representation of dates and times

ISO 8859
: Information technology – 8-bit single-byte coded graphic character sets

ISO 9075
: Information technology – database languages – SQL

ISO 10646
: Information technology – Universal Multiple-Octet Coded Character Set

ISO 23950
: Information retrieval – application service definition and protocol specification

2 Other Guidelines

90/270/EEC
: European Commission “Display Screen Equipment Directive”

BSI DISC PD 0008
: Code of Practice for the Legal Admissibility and Evidential Weight of Information Stored Electronically

BSI DISC PD2000-1:1998
: A Definition of Year 2000 Conformity Requirements (available from http://www.bsi.global.com)

3 Accessibility Guidelines

SPRITE-S2 initiative
ACCENT – Accessibility in ICT Procurement
(http://www.statskontoret.se/accenteng.htm)

W3C Web Content Accessibility Guidelines
(http://www.w3.org/TR/WAI-WEBCONTENT)

Microsoft Official Guidelines for User Interface Developers and Designers
Chapter 15, Special Design Considerations, Accessibility
(http://msdn.microsoft.com/library/books/winguide/ch15c.htm)

4 Long Term Preservation Guidelines

InterPARES project (http://www.interpares.org)

Preserving Access to Digital Information (PADI) project
National Library of Australia (http://www.nla.gov.au/padi/)

UK Public Record Office
Management, Appraisal and Preservation of Electronic Records
Guidelines, see particularly volume 2 chapter 5
(http://www.pro.gov.uk/recordsmanagement/eros/guidelines/default.htm)

Reference Model for an Open Archival Information System (OAIS)
draft intended to become an ISO standard, (available at time of writing at
http://www.ccsds.org/documents/pdf/CCSDS-650.0-R-1.pdf)