

**Functional Requirements**  
*for*  
**Electronic Records Management Systems**

**1 : Statement of Requirements**

November 1999

**Electronic Records Management Systems**

This Statement of Functional Requirements is one of the outcomes of an Invest to Save Budget project, which aims to develop cross-government requirements for electronic records management systems, and to evaluate available software products against these requirements.

The project is led by the Public Record Office, in conjunction with the Central Computing and Telecommunications Agency (CCTA), with the participation of the following departments and agencies:

Ministry of Defence  
HM Treasury  
Inland Revenue  
Department of Health  
Medical Research Council  
Department for Education and Employment

Court Service  
Crown Prosecution Service  
Treasury Solicitors Department  
Department of Social Security  
Department of the Environment,  
Transport and Regions

# Contents

<b>Introduction</b> .....	<b>5</b>
<b>Section A: Core requirements</b> .....	<b>11</b>
<i>Rationale for section A</i>	
1: <i>Record organisation and fileplan structure</i> .....	14
2: <i>Declaration and sustainability</i> .....	18
3: <i>Retention and disposal</i> .....	23
<b>Section B : Additional requirements</b> .....	<b>31</b>
<i>Rationale for section B</i>	
4: <i>Access management</i> .....	34
5: <i>Audit and authentication</i> .....	39
6: <i>Hybrid folder management</i> .....	43
<b>Section C : Supporting system requirements</b> .....	<b>47</b>
<i>Rationale for section C</i>	
7: <i>Document management facilities</i> .....	49
8: <i>Advanced search and retrieval</i> .....	50
9: <i>Bulk import</i> .....	51
<b>Section D : Informative system requirements</b> .....	<b>53</b>
<i>Rationale for section D</i>	
10: <i>Non-functional requirements</i> .....	53
11: <i>Technical standards</i> .....	56
12: <i>Documentation, consultancy and training</i> .....	58



# Introduction

## Electronic records management

All organisations need to keep records of business decisions and transactions to meet the demands of corporate accountability. In the government sector there are specific public accountability requirements as well as the need to comply with public records legislation. A record is evidence of an activity or transaction, and demonstrates accountability. Records are created by the day-to-day work that takes place in government; they need to be captured, managed and safeguarded in an organised system in order to retain their value.

The use of information and communication technology is transforming the way work is carried out in government organisations, leading to a much greater dependency on electronic records. This transition to a fuller electronic environment presents both opportunities and challenges. While paper records will continue to exist and be generated for the foreseeable future (and the means and systems for their management are well established), there is a general concern about the ability of government to manage and preserve those electronic records that are needed to support policy-making, casework and the delivery of services, and to meet accountability and archival obligations.

Electronic records management systems are needed to assist government organisations in applying records management practices to electronic records. Electronic *document* management helps organisations to exploit information more effectively and support the immediate operational requirement for business information. Electronic *records* management supports the medium to long term information needs of the business, building and maintaining the corporate memory. It manages a corporate filing structure to which records are classified, the integrity and reliability of records once they have been declared as such, and explicit disposal schedules which determine how long records should be kept and how they should eventually be disposed of – for some records by permanent preservation in the national archive.

An electronic records management system should be capable of managing electronic records throughout their lifecycle, from capture and declaration through ‘trusted record-keeping’ to eventual destruction or permanent preservation, while retaining integrity, authenticity and accessibility. Often, electronic records management requirements are not sufficiently recognised in determining the functional requirements for new information management systems and in the development of information strategies. This document sets out generic requirements for an electronic records management system.

## The rôle of this document

This Statement of Functional Requirements has been produced as part of a wider project, which intends to assess currently available software packages against the needs expressed here. This project is led by the Public Record Office working in conjunction with the CCTA, and with the participation of eleven other government departments and agencies. A working group of members from all these organisations has debated and developed these generic requirements. They are published here for use by government departments and agencies who are developing their own detailed specifications and requests for proposal.

**These generic requirements are not a full specification.** They form a baseline which sets out, in the mandatory parts of the requirement, the minimum necessary to undertake credible electronic records management. The statement also contains desirable requirements whose inclusion will provide an improved quality of electronic records management. Clearly, each

government department or agency wishing to make use of these requirements will have its own specialist needs, and will be approaching the implementation of electronic records management from an existing situation. There will always be a need for departments and agencies to tailor these requirements to their own situation by:

- adding specialist needs which are not covered at this generic level
- selecting from alternative requirements according to corporate policy and practice
- assessing whether any requirements listed here as *desirable* are *mandatory* for their individual needs
- evaluating which of the requirements listed here as *desirable* are *highly desirable* for their individual needs.

#### *Non-functional requirements*

In particular, departments will need to make their own assessment on the relative importance of non-functional requirements, and the technical operating environment in which electronic records management will be situated. The functional requirements which form the bulk of this document are intended for use by a wide range of departments and agencies – large or small, centralised or geographically dispersed, LAN-based or Intranet-based, with or without existing document management facilities, and so on – whose technical and operating needs will vary considerably. An outline of non-functional requirements is included here as an informative (rather than normative) section; departments will need to consider their own needs for:

- size, scalability, numbers of users
- performance factors and response times
- usability factors
- existing technical operating environment
- training and installation consultancy needs
- applicable technical standards.

The functional requirements make as few assumptions as possible about the software, hardware and network environment in which they will operate.

#### *Toolkit*

This document is intended as a benchmark and toolkit, which can be used by a wide range of government organisations to generate many more specialised versions of the Statement of Requirements, rather than simply copying verbatim. Using the document in this way, departments can benefit from:

- the substantial critical thinking and discussion from the inter-departmental working group of records specialists which has gone into its production
- an explicit framework of requirements to react against, which maps out the territory of electronic records management
- an assurance of consistency with the guidance on electronic records produced to date by the Public Record Office.

It is hoped that use of these requirements will foster commonality and compatibility of electronic records management systems between government departments and agencies, consistent with exchange of electronic records and joint working arrangements; and that it will encourage the software supplier industry to develop appropriate products towards a growing market in UK government for this type of application.

## Structure of the Requirements

The Statement of Requirements is structured in four sections. This structure is designed to highlight the specific features of electronic records management which distinguish it from other applications – the key features which are central and make it different. These key features will need to be supported by additional functionality that is more general and may be used by other application areas than electronic records management – for example, access management controls, and document capture facilities. The most pertinent additional functions are in section B and the more general supporting functions in section C. Non-functional requirements are outlined in section D.

For the key electronic records management features, the requirements are expressed in a detailed and specific form; for the most general supporting features the requirements are expressed at a higher level. This is not because they are less important from an overall corporate perspective – but simply because they are more general, they are already more widely understood and documented, and it is not necessary to repeat that work here. Many departments may already have some of these elements in place; others may not require all of them. The purpose of this document is to cast the spotlight on electronic records management requirements, and encourage departments to build these into a broader information management landscape.

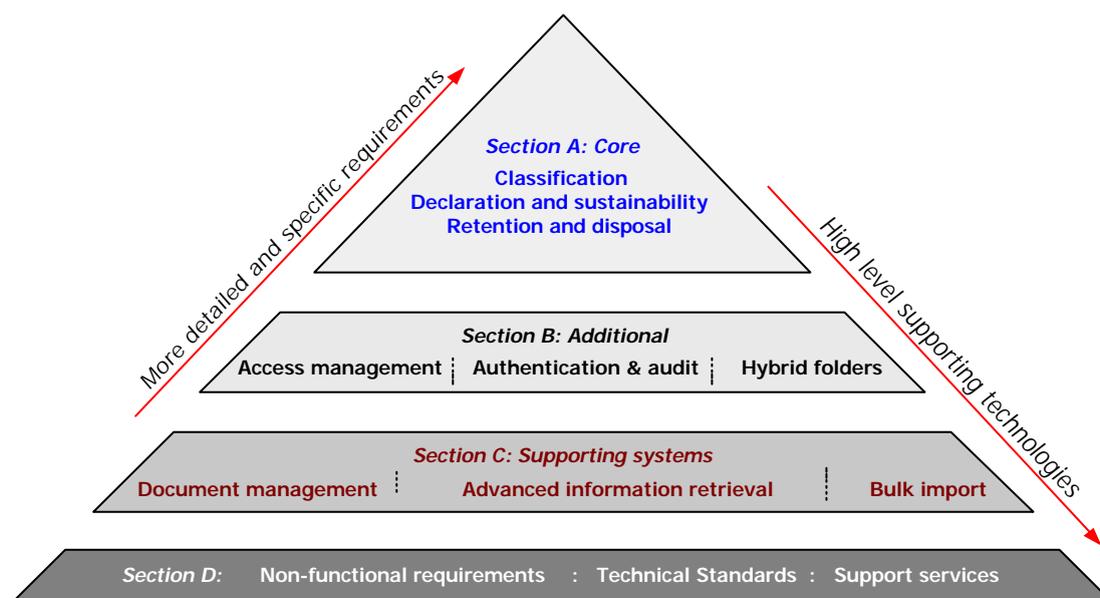


Fig. 1 : Relationship of sections in the Statement of Requirements

**Section A** deals with core electronic records management requirements: *record organisation and fileplan structure* – the ability to classify and group like records together; *declaration and sustainability* – the ability to make and maintain a record; and *retention and disposition* – the ability to set and carry through disposal schedules. All three components are essential for any electronic records management system; systems that do not possess these minimum level of requirements cannot be regarded as sound electronic records management systems. Each component is expressed as minimum and desirable requirements.

**Section B** deals with additional requirements – *access management* controls, *authentication and audit*, and the management of *hybrid folders* (combined paper and electronic folders). These are features that all departments will need to some extent (with perhaps the exception of hybrid folder management) to make effective use of electronic records; but some will be required to a greater degree than others and are features that may be delivered in varying architectures. It should be noted that a minimum level of access control and audit facilities are considered essential components of an electronic records management environment, however delivered. Each component is expressed as minimum and desirable requirements.

**Section C** deals with optional functions which are features that some departments will want and other will not, either because they already have them or because they are not relevant in their individual context.

**Section D** deals with non-functional requirements and the technical operating environment, and is informative only.

## Terminology

In the numbered requirements which follow in sections A to C, the following terminological conventions are used:

- the term “**must**” is used in each minimum requirement, to mean:
  - ≡ The ERMS must comply with all statements which follow use of the term “must” within the same numbered requirement, in order to meet this itemised requirement; and in order to meet the minimum requirements for this section or sub-section.
- the term “**should**” is used in each desirable statement, to mean:
  - ≡ An ERMS should desirably comply with all statements which follow use of this term within the same numbered requirement, and must do so to fully meet this itemised requirement; but it is not necessary to do so in order to meet the minimum requirements for this section or sub-section.
- the term “**should**” is occasionally followed by the term “**must**” to mean:
  - ≡ An ERMS should desirably offer the function or facility described, and where it does it must also fulfil the qualifying criteria defined by use of the term “must” to be compliant with this desirable requirement.
- the term “**Where ...**” is occasionally used in conjunction with the term “**must**” in the following format, to mean:
  - ≡ Where an ERMS provides a particular function, or implements a function in a certain defined manner, it must fulfil the criteria defined by use of the term “must” to meet the minimum requirements for this section or sub-section.

## Reference Document

This *Statement of Functional Requirements* is supported by an accompanying *Reference Document*. The Reference Document provides formal definitions of terms and concepts which are used in the requirements statement, and should be consulted where any questions of interpretation arise. Where it is explicitly referred to by a numbered Requirement, the cited portion of the Reference Document should be treated as an explicit context for the requirement itself.

The Reference Document includes:

- a glossary of terms
- an entity-relationship model for records management entities used in these requirements, and an explanatory commentary
- an entity life history for an electronic folder, and an explanatory commentary
- example disposal schedules
- an entity life history for an electronic record, and an explanatory commentary
- a security and access model and explanation of terms, describing control of access to electronic records
- an access/rôle matrix to describe the user rôles concept, describing control of access to system functions
- baseline metadata for electronic folders, parts, electronic records and users.



## **Section A : Core requirements**

### **Rationale**

This section sets out the core requirements for an electronic records management system in some detail. There are three main areas of requirement:

- the ability to build and maintain a fileplan structure, consisting of a hierarchy of folders that group together electronic records for management and access, and to which all records are classified
- the ability to declare an electronic document as a corporate record, and to maintain its integrity as an authentic representation of a business action or decision
- the ability to consistently manage the retention and disposition of folders of electronic records, retaining what should be kept and disposing of what should not.

These three areas are essential to any electronic records management system.

#### *Records organisation and fileplan structure*

It will be necessary to place electronic records into cognate groups for access, management, and eventual disposal.

Electronic records will need to be ordered and organised to enable the complete and reliable retrieval of a complete group of records which relate to the same business activity, case or theme, so that the context of an individual record and the narrative of a sequence of records is preserved.

Electronic records need to be organised to facilitate management of a group of related records as a single unit, for purposes of scheduling, review, preservation and destruction, so that a management process is reliably applied to all records in the group at the same time.

These groups of electronic records are called folders; folders are the building blocks of a structured corporate fileplan. Folders are usually arranged in a hierarchical structure which reflects and supports the business activities of an organisation. Specific scheduling and management characteristics will be attached to every individual folder or group of folders, according to the record-keeping requirements of the business process which they represent.

#### *Declaration and sustainability*

It will be necessary to declare electronic records that are created or acquired to support business processes, and when this happens they must be managed and maintained as corporate records.

Electronic documents will be declared as corporate electronic records either at the time of creation or at a later date. Corporate policy and the record-keeping requirements of business processes will determine which records should be declared, and when. It is essential that the necessary record components, structure and metadata have been captured to ensure the record is a reliable and authentic representation of the business activity or transaction.

It will be necessary to sustain electronic records over time as a valued corporate asset, in a manner that retains their reliability and integrity for as long as they are required, preserving their value as a corporate record. This will include prevention of changes to the content or

context to retain authenticity, and continued maintenance in an appropriate format to retain accessibility.

*Retention and disposal*

Every electronic record will be allocated to a folder at the time of declaration, and will be controlled by the disposal schedule allocated to that folder. Disposal schedules define actions to be taken on all records within folders to which they are allocated, and consist of a retention period and disposition instructions. Disposition instructions may result in review, transfer to an archive for permanent preservation, or destruction, and will be initiated by fulfilment of the retention period conditions.

The record-keeping requirements of existing records may need to be reviewed from time to time, where these are affected by changes in the external environment or changes in understanding of the long term value of particular groups of records. In particular, at the folder level, decisions may need to be made relating to an adjustment in retention within the organisation, to the sensitivity of the contents, or to selection for permanent preservation.

It will be necessary to export (transfer) some folders of records to the Public Record Office or other appointed place of deposit for permanent preservation; and it may be necessary to export folders to another ERMS. Transfer will include both *record content* and descriptive material relating to *record context*, such as file structure, folder and record metadata. To support the process of review and preparation for transfer, it will be necessary to add free-text annotations as metadata at the folder level – for example, reasons for a review decision; the destination class reference for records to be transferred – which may be used to develop archival finding aids.

It will be necessary to remove groups of folders or individual folders from the system following a decision to expunge them. This decision may be initiated by activation of a disposal schedule instruction which indicates destruction, or by confirmation of successful transfer to the Public Record Office.

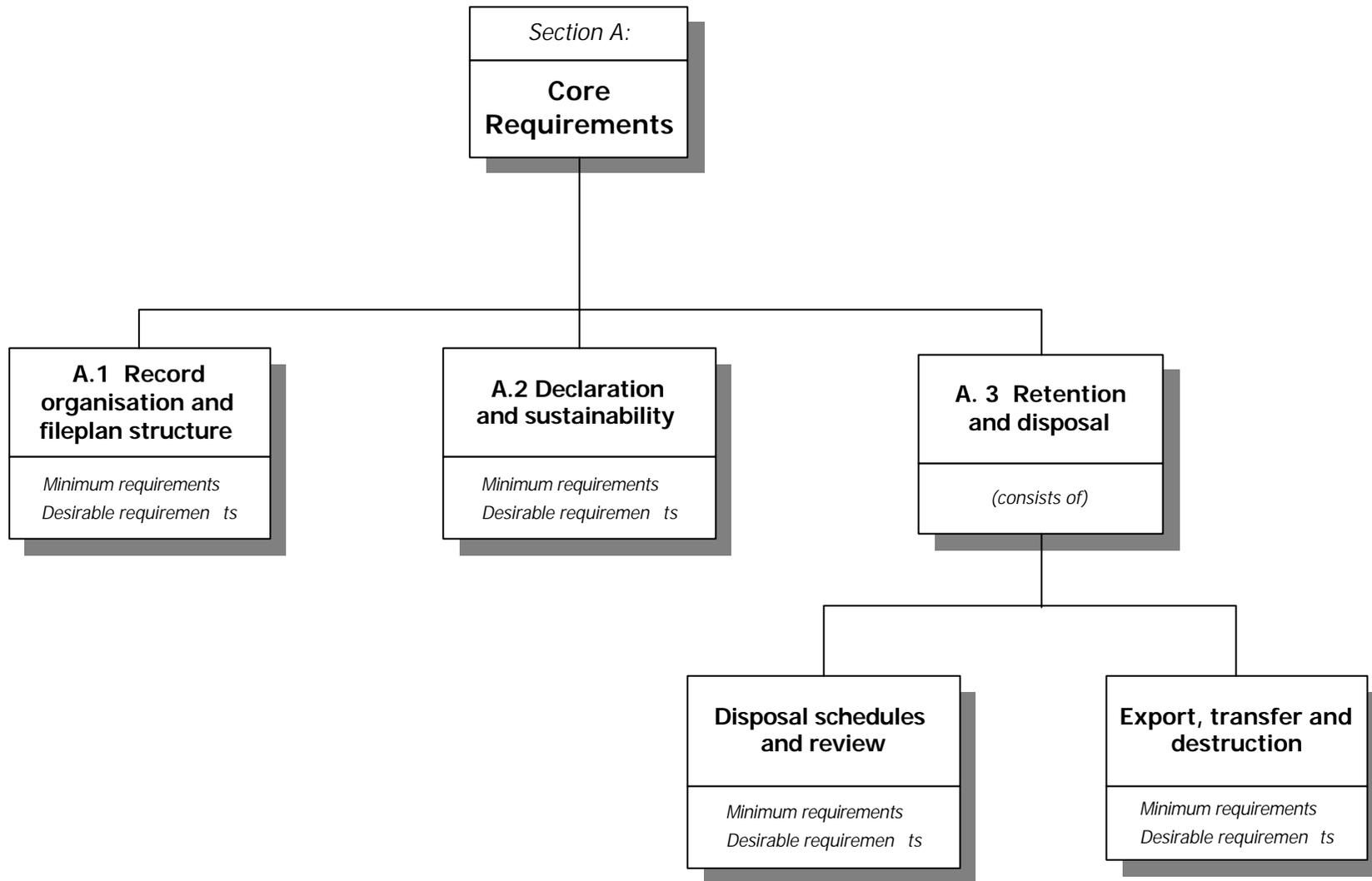


Fig. 2: Structure of Section A

## 1 : Record organisation and fileplan structure

### High level requirements

- The ERMS must support the creation, maintenance and adaptation of an electronic fileplan to which all electronic records will be classified at the time of declaration, by allocation to a folder within the fileplan.
- The ERMS must provide consistent and predictable structuring principles for the electronic fileplan, including at least a three-level hierarchical structure, and support for both numerical coding and a text-based naming system.
- The ERMS must support the concept of open and closed electronic parts, as subsidiary and discrete sub-groupings within an electronic folder, delimited according to rules specified at installation; and the concept of open and closed electronic folders inclusive of their constituent parts.
- The ERMS should be capable of classifying an electronic record by multiple entries within a folder structure and must then manage the referential integrity of all index data.
- The ERMS must be able to retrieve electronic records by search of record metadata, and electronic folders or groups of folders by search of folder metadata; and must enable navigation through the folder structure.
- The ERMS must be able to retrieve a complete electronic folder and all the electronic records which have been allocated to the retrieved folder, as a whole group, and present these distinctly from any other retrieved folder.

### Detailed requirements

#### *Minimum requirements*

- A.1.1. The ERMS must support an electronic fileplan, consisting of electronic folders and electronic folder parts, to one or more of which all electronic records must be classified by completion of the process of declaration.
- A.1.2. The ERMS must support a hierarchical electronic fileplan, with a minimum of three electronic folder levels below the root level.

An electronic folder must link, in a parent-child relationship, *either* to one or more electronic folders at a lower level, *or* to one or more electronic parts at a lower level, *but not* to both folders and parts.

An electronic part must only contain electronic records (or electronic records and markers if hybrid folder management is supported – *see section B6*).

- A.1.3. The ERMS must provide at least two naming principles for electronic folders in the fileplan:
  - a mechanism for allocating a structured numerical reference code to each electronic folder

- a mechanism to allocate a textual folder title for each electronic folder
- both of which principles which can be separately applied in the same system.
- A.1.4. The ERMS must ensure that each electronic folder within the fileplan can be uniquely identified by the full path of the numerical reference and text name (that is, the full name or code including all folder names or numerical codes at a higher level); but allow repetition, at different points in the fileplan, of a folder name which represents only one segment of a full path name<sup>1</sup>.
- A.1.5. The ERMS must support the initial construction of an electronic fileplan (as part of the installation process) prior to, and in readiness for, the declaration or import of electronic records.
- A.1.6. The ERMS must allow the addition of electronic folders at any point within the fileplan structure, and record the date of opening of the folder; and should be able to restrict this ability to authorised users.
- A.1.7. The ERMS must allow the addition of electronic parts to any electronic folder which is not closed, and should be able to restrict this ability to authorised users.
- A.1.8. The ERMS must support the concept of open and closed electronic parts; with the exception described in *A.1.11*, only the most recently created part within a folder will be open and all other parts within that folder will be closed.
- A.1.9. The ERMS must prevent the addition of electronic records to a closed part.
- A.1.10. The ERMS must allow an electronic folder to be closed, by a records administrator, to prevent the further addition of electronic records or parts to that folder.
- A.1.11. The ERMS must allow an authorised user (at records administrator level and above) to open a previously closed folder or part for the addition of records, and subsequently to close that folder or part again.
- A.1.12. The ERMS must allow an electronic folder and its parts, or a hierarchical group of folders and their parts, to be relocated to a different position in the fileplan by a records administrator, and must ensure that all electronic records already allocated to that folder and part remain so allocated following the relocation.
- A.1.13. The ERMS must allow an electronic record to be re-located to another electronic folder part, and must be capable of restricting this ability to records administrator level.
- A.1.14. The ERMS must prevent the deletion of an electronic folder and its contents at all times, with the exceptions of:
- destruction in accordance with a disposal schedule – *see section A3*
  - deletion by a systems administrator as part of an audited procedure.

---

<sup>1</sup> For example: the path *Contracts : Company name : Correspondence* is unique, but the final segment may be repeated in the path *Regional plan development : Public consultation : Correspondence*

- A.1.15. The ERMS must support the use of folder level metadata<sup>2</sup>, and must restrict the ability to amend folder metadata to records administrator level and above.
- A.1.16. The ERMS must allow an electronic record to have multiple entries in the fileplan, each entry being in a different electronic folder.
- A.1.17. Where multiple entries are achieved by use of a pointer system, the ERMS must be able to manage the integrity of all pointers or references, to ensure that:
- all references or pointers link to a valid destination
  - removal (by export, transfer or destruction) of a destination also removes all linking references, unless an intervention action is taken as in A.3.34.
  - change in location of a destination also redirects any linking references.
- A.1.18. The ERMS must be able to search for and retrieve a complete electronic folder, or folder part, and all its entries, and display all, and only, those entries in the context of that folder as a discrete group and in a single retrieval process – (that is, provide 100% recall and 100% precision of the entries in a specified folder or part).
- A.1.19. The ERMS must be able to search for, retrieve and display a set of electronic records taken from many different folders by specifying values to be searched for in electronic record metadata.
- A.1.20. The ERMS must be able to search for, retrieve and display an electronic folder by all implemented naming principles, including:
- a folder title text
  - a folder numerical reference code.
- A.1.21. The ERMS must support browsing and graphical navigation of the fileplan structure, and the selection, retrieval and display of electronic folders and their contents through this mechanism.

*Desirable requirements*

- A.1.22. The ERMS should support multiple electronic fileplans.
- A.1.23. The ERMS should support a distributed electronic fileplan which can be maintained across a network of electronic record repositories.
- A.1.24. The ERMS should support an optional folder naming mechanism that is based on controlled vocabulary terms and relationships drawn from a thesaurus, and that is compliant to ISO 2788.
- A.1.25. The ERMS should support the allocation of controlled vocabulary terms and relationships, as descriptive folder metadata subject terms in addition to the folder name and numerical reference code, that is compliant to ISO 2788.
- A.1.26. When creating a new electronic folder in a fileplan which uses a structured numerical coding reference, the ERMS should automatically generate the next sequential number available at that position within the fileplan.

---

<sup>2</sup> Baseline record and folder metadata are listed in the Reference Document at p.35-39.

## SECTION A : CORE REQUIREMENTS

---

- A.1.27. The ERMS should validate the name – numerical code or textual title – as it is allocated to a newly created electronic folder, according to validation rules specified by the systems administrator.
- A.1.28. The ERMS should support the ability to enter a short free-text description of each electronic folder as an element of folder metadata.
- A.1.29. The ERMS should support the creation of relational links (that is, ‘see also’ type links) between folders of related interest.
- A.1.30. The ERMS should be able to automatically close an electronic folder part on fulfilment of specified criteria to be defined at configuration, including at least:
- parts 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 last addition of an electronic record to that part
  - the number of electronic records which a part contains
  - the physical size (in disk storage terms) of the electronic records contained in a part.
- A.1.31. The ERMS should support the ability to create multiple entries for electronic records in different electronic folders without physical duplication of the electronic record itself.
- A.1.32. The ERMS should support reporting tools for the provision of statistics to the records manager on aspects of activity within the electronic fileplan, including:
- the number of electronic folders created within a given period
  - the number of electronic parts opened and closed within a given period
  - the number of electronic records added to folders within a given period, stratified by user.

## 2 : Declaration and sustainability

### High level requirements

- The ERMS must enable electronic documents arising in the course of business to be declared as electronic records by an end user, by either:
  - providing facilities for the capture of electronic documents itself
  - providing integration with a different capture environment.
  
- The ERMS must be able to take into the electronic record management environment :
  - the content of the electronic record including its presentational form or rendition
  - the structure 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)
  - information about the electronic document, for example, the file name and the date of creation - the document metadata
  - information about the context in which the electronic record was originated and declared, for example its originator(s) and the date of declaration - the record metadata.
  
- The ERMS must prevent any changes to:
  - the content of the electronic record
  - the metadata of the electronic records (except where specified)once declared as a record, and must maintain electronic record content and metadata together in a tightly-bound relationship.
  
- The ERMS must maintain access to and visibility of the electronic record content, including the logical content, structure and formatting, over time and through generations of office application software; for example, by use of a multi-format viewer application.

### Detailed requirements

#### *Minimum requirements*

- A.2.1. The ERMS must ensure that electronic documents can be captured, so that they can be declared and stored as electronic records, by one of the following:
  - providing electronic document capture facilities as an integral feature of the ERMS
  - integrating the ERMS with a document management system which provides electronic document capture facilities, and which can make captured documents available to the ERMS.

## SECTION A : CORE REQUIREMENTS

---

- A.2.2. The ERMS must support the process of declaration, in which an electronic document is marked as a formal electronic record and is associated with one or more folders in the electronic fileplan by an end user.
- A.2.3. The ERMS must at all times prevent the deletion of any electronic record that has been declared, with the exceptions of:
- destruction in accordance with a disposal schedule – *see section A3*
  - deletion by a systems administrator as part of an audited procedure.
- A.2.4. The ERMS must prevent any amendment to the content of any electronic record, by any user.
- A.2.5. The ERMS must be able to ensure the capture of, declare and manage the following types of electronic documents which have been created or received in the course of business :
- word processing documents
  - documents produced by text editors
  - spreadsheets
  - e-mail messages
  - e-mail messages with attachments
  - complete 'web pages', with all components
  - presentations
  - desktop publishing documents
  - PDF format documents
  - document images from a scanning system
  - single static images and graphics in common formats.
- A.2.6. Where electronic records are constructed of more than one component, the ERMS must be able to ensure the capture of, and to declare and manage electronic records in a way that retains the relationship between the constituent components, retains their structural integrity, and supports later integrated retrieval, display, management and disposal of the electronic record as a whole unit. In particular, the ERMS must ensure the capture of, and be able to declare and manage:
- an e-mail message with one or more attachments, maintaining e-mail text and attachments as a single electronic record
  - a 'web page' consisting of text and image components, retaining the relationships between all components as a functional unit, and maintaining them as a single electronic record.
- A.2.7. The ERMS must ensure the capture of, and be able to declare, electronic records in their native format.

- A.2.8. The ERMS must ensure the capture of all metadata elements<sup>3</sup> specified at systems configuration, and retain them with the electronic record in a tightly-bound relationship at all times.
- A.2.9. The ERMS must allow:
- the metadata element set for electronic record logical types to be selected when configuring the ERMS at implementation
  - each selected metadata element to be defined as either mandatory or optional (except where the system requires metadata elements to be mandatory)
  - reconfiguration of the selected metadata set if necessary.
- A.2.10. The ERMS must allow the definition of an unlimited number of user-defined metadata elements.
- A.2.11. The ERMS must be capable of managing:
- metadata acquired directly from the document-creating application package or operating system where feasible
  - metadata acquired from the user at the time of capture or declaration
  - metadata generated by the ERMS at the time of declaration.
- A.2.12. The ERMS must prevent any amendment of metadata generated directly from the application package, the operating system or the ERMS: for example, e-mail transmission data.
- A.2.13. The ERMS must restrict the amendment of user-generated metadata to:
- the owner and originator of the electronic record concerned
  - the records administrator, where an owner is not identified after the record has been declared.
- A.2.14. The ERMS must record the date and time of declaration as a metadata element.
- A.2.15. The ERMS must support the definition and application of validation rules for each metadata element, at a minimum including validation of:
- date formats
  - numeric formats
  - valid fileplan location.
- A.2.16. The ERMS must ensure that all electronic records are associated with one or more entries in the electronic fileplan on completion of declaration.
- A.2.17. The ERMS must be able to allocate a unique identifier<sup>4</sup> to each electronic record on declaration, that serves to identify the unique record from the point of declaration throughout the remainder of its life.

---

<sup>3</sup> Baseline record and folder metadata are listed in the Reference Document at p.35-39.

<sup>4</sup> Note that this is a unique number globally within the ERMS.

- A.2.18. The ERMS must retain the original document title for display and export purposes.
- A.2.19. The ERMS must be capable of assigning to each electronic record a sequence number<sup>5</sup> which is unique within each electronic folder part; use of this number to be selectable at time of implementation.
- A.2.20. The ERMS must ensure the capture of e-mail transmission data and be capable of mapping this data to electronic record metadata<sup>6</sup>.
- A.2.21. The ERMS must be able to display all the types of electronic records listed in A.2.5 in a manner that shows all the features of visual presentation and layout produced by the generating application package, and which displays all components of an electronic record together as a unit.
- A.2.22. The ERMS must be able to display all metadata associated with an electronic record.
- A.2.23. The ERMS must be able to print all types of electronic records listed in A.2.5, in the same manner as they are displayed on screen, without use of 'screen-dumping' or 'snapshots'.
- A.2.24. 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.

*Desirable requirements*

- A.2.25. In addition to those specified in A.2.5, the ERMS should be able to ensure the capture of, declare and manage the following types of electronic documents which have been created or received in the course of business:
- office documents with embedded objects from a different package, for example a word processing document with embedded spreadsheet
  - databases created in desktop office application packages
  - digital video clips
  - electronic diaries and notepads
  - project plans
  - physical data files from CAD/CAM applications
  - digital maps and plans
  - digitised sounds.
- A.2.26. The ERMS should support the ability to declare:
- an electronic document in one specified version only, when more than one version of the document exists, and hold this as an electronic record

---

<sup>5</sup> Note that this is unique within the folder, and acts as an 'enclosure number', and that it is different from the global identifier in A.2.17

<sup>6</sup> Mapping between e-mail transmission fields and baseline metadata elements is set out in the Reference Document at p.39.

- an electronic document in all existing versions, and hold all of these as a single electronic record.
- A.2.27. The ERMS should be able to link an instance of an electronic record (that is, a redaction of the original record from which portions of content have been masked) 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.
- A.2.28. The ERMS should support the ability to define different logical types for electronic records, and the allocation of different metadata elements sets for each logical type. Examples of distinct types are:
- pre-defined forms
  - committee minutes
  - letters.
- A.2.29. The ERMS should support the ability to allocate one or more controlled vocabulary terms to an electronic record by integration with an ISO 2788 compliant thesaurus.
- A.2.30. The ERMS should ensure the capture of an 'intelligent' version of an e-mail message address, where one is associated with the original message; for example, *'John Smith'* rather than *js042@aol.com*.
- A.2.31. The ERMS should provide support for decisions on the allocation of electronic records to electronic folders by:
- suggesting the most recently used folders by that user
  - suggesting folders which contain known related electronic records
  - suggesting folders by inferences drawn from record metadata elements: for example, significant words used in the document title.
- A.2.32. The ERMS should allow an end user to pass electronic records to a records administrator during the process of declaration, to complete the process by classification within the fileplan.
- A.2.33. The ERMS should support reporting tools for the provision of statistics to the records manager on aspects of electronic records in the ERMS, including
- the number and location of electronic records by application type and application package version
  - the number and location of electronic records by access control markings.

### 3 : Retention and disposal

#### High level requirements

- The ERMS must be capable of allocating a disposal schedule to all folders and folder parts which exist in the electronic fileplan, that can be initiated by:
  - time-based criteria
  - event-based criteria
  - combined time and event-based criteria

and which determine disposition actions to be taken on the folder or part to which it is allocated.

- The ERMS must support separate disposition instructions which include:
  - further retention and review at a later date
  - transfer to the Public Record Office for permanent preservation
  - destruction.
- The ERMS must support the application of disposal schedules as they come into force, alerting and prompting the records management staff as necessary, and carrying out consequent actions within the system.
- The ERMS must support the review process and a re-allocation of disposal schedules, and allow the progressive addition of metadata elements recording annotations resulting from the review process.
- The ERMS must be able to export:
  - electronic record content and structure
  - metadata describing the electronic records
  - information about the folder structure information
  - information about the position of records in the folder structureselectively and in bulk, without degradation of content or format, and without loss of any element of the record, including linkages, attachments and embedded objects.
- The ERMS must provide facilities to destroy completely groups of folders and individual folders according to their scheduling, and record the fact of destruction in the ERMS.

## Detailed requirements

### Disposal schedules and review

#### *Minimum requirements*

- A.3.1. The ERMS must enable the allocation of a disposal schedule<sup>7</sup> to every electronic folder in the electronic fileplan, that will be applied to all the contents of that folder, which must be managed according to the disposal schedule of that folder (unless a separate disposal schedule for its constituent parts has been allocated).
- A.3.2. The ERMS must enable the allocation of a disposal schedule to a group of electronic folders in the electronic fileplan; all folders descendent from that point in the hierarchy of the fileplan (with exception in the case of A.3.3) must be managed according to the disposal schedule for that group of folders.
- A.3.3. The ERMS must enable a disposal schedule to be allocated to a specific folder that can take precedence over a disposal schedule allocated at a higher point in the hierarchy for this folder.
- A.3.4. The ERMS must allow the allocation of a separate disposal schedule to an individual part within an electronic folder; where an individual part is not allocated a distinct schedule, the schedule for the folder must come into force.
- A.3.5. The ERMS must ensure that where an electronic record has multiple entries in more than one electronic folder, and these folders have different disposal schedules, the records administrator is notified of this conflict prior to disposition instructions being carried out.
- A.3.6. The ERMS must be capable of restricting the ability to allocate and amend disposal schedules to records managers.
- A.3.7. The ERMS must support disposal schedules which consist of:
- a retention period, and
  - a set of disposition instructions.
- A.3.8. The ERMS must support the allocation of a retention period which can be expressed as:
- the passage of a period of time
  - the occurrence of a specified event
  - the passage of a period of time following a specified event.
- A.3.9. The ERMS must support types of 'passage of a period of time' in a retention period which can be expressed as a period of either:
- a number of whole months, from one to eleven months
  - a number of whole years, from one to 100 years.

---

<sup>7</sup> Example disposal schedules are shown in the Reference Document at p.21.

## SECTION A : CORE REQUIREMENTS

---

- A.3.10. The ERMS must support types of ‘occurrence of a specified event’ in a retention period which include:
- opening date of a electronic folder or part
  - closing date of an electronic folder or part
  - last addition (that is, date of declaration) of an electronic record to an electronic folder or part
  - last retrieval of an electronic record from an electronic folder or part.
- A.3.11. The ERMS must support types of ‘occurrence of a specified event’ in a retention period which occurs outside the knowledge of the system, and must enable a records administrator to record the fact that a specified event has occurred.
- A.3.12. The ERMS must automatically track retention periods that have been allocated to electronic folders within the system, and initiate the disposal process once their specified conditions are fulfilled.
- A.3.13. The ERMS must support the allocation of disposition instructions as part of a disposal schedule which include:
- review of the electronic folder and contents
  - export of the electronic folder and contents for permanent preservation
  - destruction of the electronic folder and contents.
- A.3.14. The ERMS must alert the records administrator to disposal schedules as they come into force and seek confirmation before implementing disposal actions; and on confirmation must be capable of initiating the disposal actions specified in *A.3.13*.
- A.3.15. The ERMS must enable the amendment by a records manager of a disposal schedule allocated to any electronic folder or part, or a group of folders, at any point in the life of the folder or part.
- A.3.16. The ERMS must enable a records manager to view and print:
- a list of all disposal schedules
  - a list of all electronic folders and parts to which a specified disposal schedule is allocated
  - the disposal schedule(s) applied to all folders and parts below a specified point in the hierarchy of the electronic fileplan.
- A.3.17. The ERMS must be capable of identifying electronic folders and parts which are scheduled for review within a given time period of, as a minimum, between one and twelve months, according to user-defined criteria.
- A.3.18. The ERMS must enable the allocation of a review decision to an electronic folder or part, or a group of folders, which is undergoing review, including:
- re-allocation of a further disposal schedule as listed in *A.3.13*
  - selection for permanent preservation by transfer (export) to the Public Record Office
  - immediate destruction following completion of review.

*Desirable requirements*

- A.3.19. The ERMS should support the use of standard terms for the expression of disposal schedules, provide validation facilities for the creation, amendment and allocation of these terms, and enable global changes to be made to these schedules.
- A.3.20. When moving electronic folders or groups of folders between branches of the electronic fileplan, the ERMS should enable the destination schedule to optionally replace the source schedule.
- A.3.21. The ERMS should enable the reviewer to complete a metadata element to be held with the electronic folder or groups of folders being reviewed, as a free-text comment on the review process<sup>8</sup>.
- A.3.22. The ERMS should provide, or support the ability to interface with, workflow facilities to support the scheduling, review and export/transfer process, by tracking:
- progress of the review – awaiting, in progress, reviewer details and date
  - awaiting disposal as a result of a review decision
  - progress of the transfer process.
- A.3.23. The ERMS should provide a facility to define sets of processing rules which can be applied in a checking and alerting facility to specified electronic folders and groups of folders, prior to initiation of a disposal process.
- A.3.24. The ERMS should support reporting and analysis tools for the management of retention and disposal schedules by the records manager, including the ability to:
- notify all disposal schedules which will come into force in a given period of time, and provide quantitative reports on electronic folder size and electronic record types
  - notify statistics of review decisions in a given period
  - identify, compare and review disposal schedules across the electronic fileplan
  - identify formal contradictions in retention and disposition across the electronic fileplan.

---

<sup>8</sup> Note this is a different metadata element from the review decision described in A.3.18

## Export, transfer and destruction

### *Minimum requirements*

- A.3.25. The ERMS must be able to support the flagging of electronic folders and groups of folders for export to another ERMS, or for transfer to the Public Record Office for permanent preservation.
- A.3.26. The ERMS must be able to identify and list electronic folders marked for permanent preservation as their disposal schedules comes into force.
- A.3.27. The ERMS must be able to export whole electronic folders of records in one sequence of operations, such that:
- the content and appearance of the 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 attachment
  - all metadata associated with an electronic record is linked to the record to which it belongs
  - all electronic records within a specific folder remain associated with that folder
  - all electronic folder and part metadata is exported and remains associated with that electronic folder and part.
- A.3.28. The ERMS must be able to export multiple entries, where an electronic folder to be exported contains a pointer rather than the physical record; at a minimum, by achieving this effect through physical duplication of records to be exported.
- A.3.29. Where an ERMS does not support the addition of metadata to electronic folders selected for export or transfer, and the sorting of folders into ordered lists, it must interface with an appropriate package (for example a report management package) for this purpose.
- A.3.30. Where an ERMS does not support the rendering of records and folders marked for transfer to the Public Record Office into an approved transfer format<sup>9</sup>, it must interface with an appropriate package or conversion utility for this purpose.
- A.3.31. The ERMS must produce a report detailing any failure completely to export electronic records and folders and associated metadata, which identifies any records allocated for transfer which have generated processing errors.

---

<sup>9</sup> At present approved transfer formats, according to appropriate record type are:

- PostScript
- SGML
- PDF
- TIFF (images)
- Delimited (e.g. Comma Separated Variable) (structured data)

These formats are subject to revision as record-generating applications become established.

- A.3.32. The ERMS must retain intact all electronic folders that have been exported or transferred, at least until confirmation of a successful transfer process.
- A.3.33. The ERMS must regularly alert the records administrator to electronic folders which are scheduled for destruction, as these fall due, and require confirmation of the action before initiating destruction.
- A.3.34. The ERMS must alert the records administrator if an electronic folder that is due for destruction contains an electronic record which has an entry in a different folder; and must pause the destruction process to allow the following remedial action to be taken:
- confirmation by the records administrator to proceed with or cancel the process
  - generation of a report detailing the record(s) concerned and all references or links for which it is a destination.
- A.3.35. The ERMS must provide facilities to enable the complete destruction of groups of folders or individual folders that have been so scheduled and confirmed, so that they cannot be restored by normal use of the ERMS or by standard operating system utilities.

*Desirable requirements*

- A.3.36. The ERMS should be able to identify and report on electronic records to be exported or transferred, which transgress the following conditions:
- where a record or folder marked for export or transfer references (i.e. points to) a record or folder which is not so marked
  - where a record or folder marked for export or transfer is referenced (i.e. pointed to) by a record or folder not so marked
- and enable the conflict to be resolved by:
- retaining a copy of the destination record within the folder
  - creating a fresh copy of the destination record and re-directing all linking references
  - removing all linking references with the destination record.
- A.3.37. When exporting specified electronic folders and records, the ERMS should enable selection of folder and record metadata required, and should export only that set of metadata.
- A.3.38. The ERMS should support the selection and export of electronic record and folder metadata, independently from record content, in a form suitable for migration to a Web-based environment, in order to support a resource discovery service.
- A.3.39. The ERMS should be able to export and transfer multiple entries (i.e. links between a physical record and its entry in more than one folder) without duplication of records.

- A.3.40. The ERMS should be able to export groups of electronic folders in one sequence of operations, such that all conditions of A.3.27 are met, and:
- the relative location of each folder in the electronic fileplan structure is maintained, so that the folder structure can be reconstructed
  - all folder metadata at higher points in the hierarchy is retained with that folder.
- A.3.41. The ERMS should enable electronic records selected for transfer to be *directly* rendered into a format approved by the Public Record Office<sup>10</sup>, in a manner which retains their content and appearance.
- A.3.42. The ERMS should provide the ability to:
- add user-defined metadata elements required for archival management purposes to electronic folders selected for transfer
  - sort electronic folders selected for transfer into ordered lists according to user-defined metadata elements
  - generate user-defined forms to describe electronic folders that are being exported or transferred.
- A.3.43. The ERMS should be capable of marking for destruction records that have been exported or transferred; destruction should not be carried out until a successful export or transfer has been confirmed.
- A.3.44. The ERMS should allow exported records to remain within (and not be deleted from) the system.
- A.3.45. The ERMS should enable the total destruction of groups of folders and individual folders that are stored on re-writable media, by completely obliterating them so that they cannot be restored by use of specialist data recovery facilities.
- A.3.46. The ERMS should enable the retention of a metadata ‘stub’ for electronic records and electronic folders that have been destroyed, which can be indexed and retrieved alongside metadata for existing records, to indicate the absence of sought items.

---

<sup>10</sup> See footnote 9.



## **Section B : Additional requirements**

### **Rationale**

This section sets out additional requirements for electronic records management systems. These functions will be required by all organisations, to maintain the integrity of electronic records, and to ensure appropriate access and use; but will be required in different degrees of sophistication by different departments and agencies, according to the nature of their business needs and current situation.

#### *Access management*

Electronic records contain evidence of business transactions and activities and may also possess personal, commercial or other sensitive information. It will be necessary to manage access to these records to ensure compliance with the regulatory environment and corporate policy, and in accordance with the security model described in the Reference Document at pages 27-30.

Access management aims to strengthen privacy and security while facilitating information sharing. Electronic records management must comply with Data Protection legislation by restricting inappropriate access and will be required to support forthcoming Freedom of Information legislation. Corporate policy will require that specific records or folders can be protectively marked in order to limit user access to individuals or specified groups; the need to control such access will usually diminish with the passing of time.

Both corporate policy and the need to retain integrity and authenticity in electronic records will require restriction of access to system functions according to user rôle.

It will be necessary to ensure that rights of access to records and to functions are granted to authorised individuals and groups, and withheld from unauthorised individuals and groups.

#### *Audit and authentication*

It will be necessary to be capable of demonstrating that electronic records have been managed according to pertinent requirements of the *Code of practice for legal admissibility*<sup>11</sup>, and that any necessary authentication has been successfully demonstrated.

An audit trail which tracks actions taken on electronic records and folders relating to declaration, access, management, preservation and disposal will be necessary to demonstrate authenticity throughout the record lifecycle.

It may be necessary to store digitally signed electronic records through time and across platforms. A digital signature will need to be verified prior to entering the record, and the details of verification recorded once it has done so. It will not be necessary to routinely verify digitally signed records once they are declared, because they will be managed within the system in a manner that ensures authenticity.

---

<sup>11</sup> *Code of practice for legal admissibility and evidential weight of information stored electronically* (DISC PD0008:1999). British Standards Institute, 1999.

*Hybrid folder management*

It is unlikely that the paper record will be completely replaced by the electronic record in the foreseeable future. Many organizations will wish to continue creating and acquiring records in paper form, and will wish to integrate management of hybrid folders which contain both paper and electronic records. In addition, it may be desirable to be aware of the existence and location of complete paper folders.

There are two alternative approaches to hybrid folder management embodied in this requirement:

- the inclusion of markers for paper records (metadata profiles of individual paper and other records) as entries within the electronic folder; this approach is most effective in a largely electronic system with a smaller number of related paper records
- the inclusion of hybrid paper folders (metadata profiles of a parallel paper folder) tightly linked with an associated hybrid electronic folder, and with the same substantive textual title and numerical reference code; this approach is more suitable for situations in which substantial portions of one logical folder are in a physical paper format.

In both cases, the markers and paper folders should be governed by the same disposal schedule as the related electronic records.

In addition, it may be necessary to be aware of the existence of a complete paper folder which has no associated hybrid electronic folder, but which is of related interest to electronic records that are held within the ERMS. In this case, minimum location metadata or a reference to a separate electronic registry management system will be adequate.

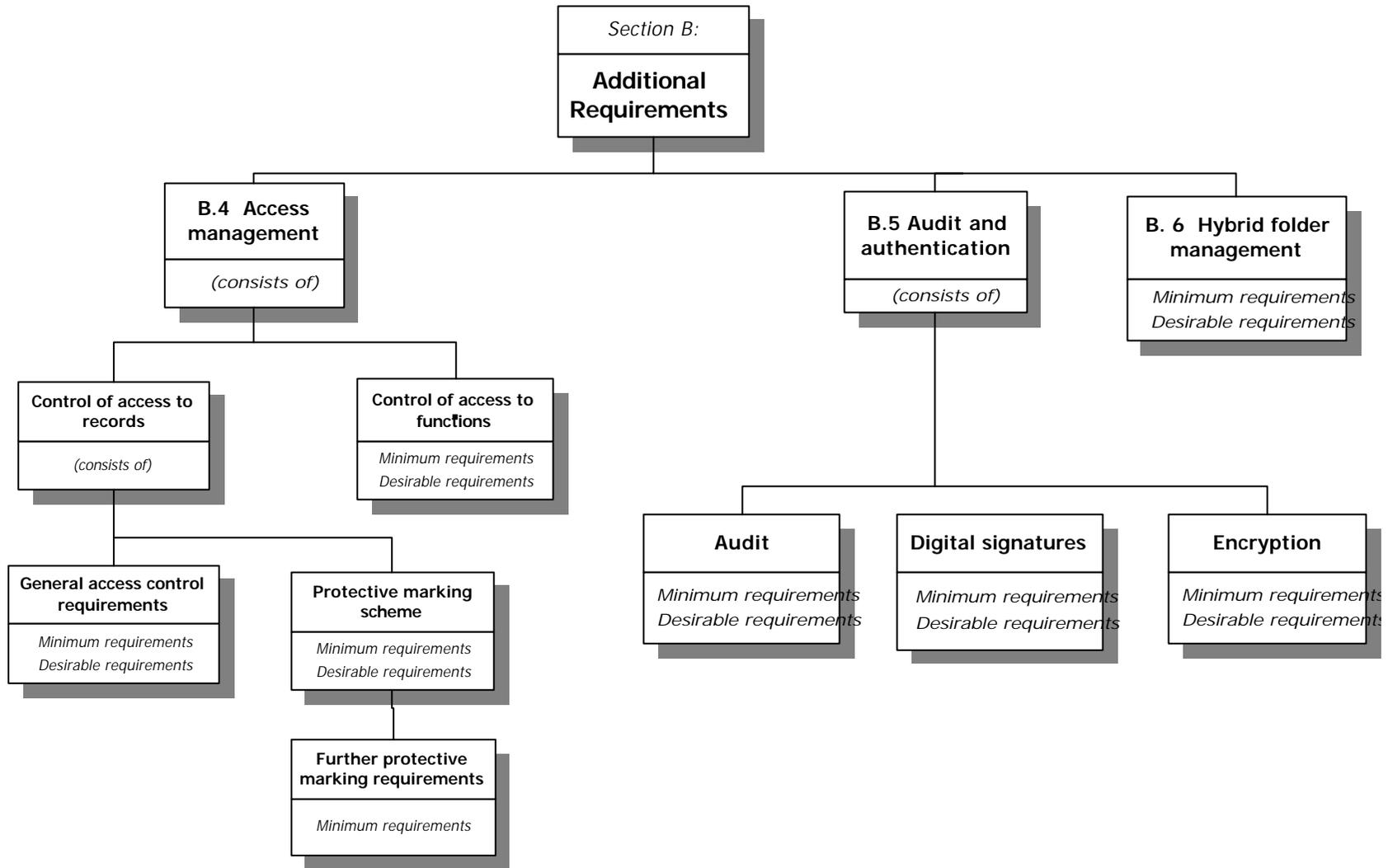


Fig. 3: Structure of Section B

## 4 : Access management

### High level requirements

- The ERMS must support control of access to electronic records and electronic folders.
- The ERMS must support a minimum protective marking scheme, which allocates security categories to records, folders and users as a means of controlling access; and should support a more extensive protective marking scheme.
- The ERMS must support control of access to electronic records and electronic folders by:
  - business or organisational grouping
  - lists of named users
  - individual owner.
- The ERMS must support the allocation of users to one or more user roles, which determine allowable user access to system functions and facilities available in the ERMS.

### Detailed requirements

#### Control of access to records

#### General access control requirements

##### *Minimum requirements*

- B.4.1. The ERMS must support the use of access control markings for:
- groups of electronic folders
  - electronic folders
  - electronic records.
- B.4.2. The ERMS must allow all users (unless otherwise restricted by functional rôle) access to all electronic folders and electronic records which are not allocated an access control marking.
- B.4.3. Where an ERMS supports a protective marking scheme, the ERMS must support a protective marking scheme as detailed in *B.4.16 – B.4.23*.
- B.4.4. The ERMS must enable the allocation of access control markings (including protective markings) as metadata elements for both electronic records and electronic folders.
- B.4.5. The ERMS must enable the addition of a *released under Freedom of Information request* metadata element, containing details of the release, to any electronic record or electronic folder.

- B.4.6. The ERMS must enable the allocation of access control markings (including protective markings) as metadata elements for each user of the system, and restrict the ability to allocate these markings to the systems administrator.
- B.4.7. The ERMS must enable, but not necessarily require, an owner<sup>12</sup> for each electronic record and electronic folder to be identified in a metadata element for that record or folder, and enable this identification to be changed at a later date as necessary.
- B.4.8. The ERMS must support the allocation of access control markings to electronic records, electronic folders and users which identify business groups; for example, work teams, organisational units.
- B.4.9. The ERMS must be able to limit access to any element of electronic records and electronic folders which have been allocated one or more access control markings only to users who have also been allocated *all* equivalent access control markings; and prevent access by users who have been allocated some, but not all, the equivalent access control markings.
- B.4.10. The ERMS must be able to limit access to an electronic record or electronic folder to a list of named users for that record or folder, and must enable an owner of a record or folder to create and maintain such a list. This form of access control marking falls within the scope of access control markings in *B.4.9*
- B.4.11. The ERMS must be able to limit access to an electronic record or electronic folder solely to an owner of that record or folder.
- B.4.12. The ERMS must support the amendment of access control markings, but retain the previous marking(s), and the date of the amendment, as an historical metadata element for that electronic record or electronic folder.
- B.4.13. The ERMS must restrict the ability to allocate and amend access control markings on electronic records and electronic folders to:
- the owner of the record or folder in all cases
  - the records manager, except where access is denied to this user (for example, as in *B.4.10* and *B.4.11*)
  - the systems administrator, where no other user has current access.

*Desirable requirements*

- B.4.14. The ERMS should support the allocation of access control markings which are valid for a specified time period, and should notify the records manager shortly prior to the termination of that period.
- B.4.15. The ERMS should include an option, selectable at time of installation, which defines the behaviour of the access control mechanism so that:

---

<sup>12</sup> Note that an owner of a record may be a different user than the creator of a record. Where a conflict exists between the owner of a folder and the owner of a record contained within that folder, the owner of the folder will take precedence.

- *either* a user who is not allowed access to an electronic record or folder can never find out that it exists by means of the ERMS (i.e. the user can never see its metadata, in a search result list or at any other time)
- *or* a user who is not allowed access to an electronic record or folder can find out that it exists by means of the ERMS (i.e. the user can see its metadata, e.g. in a search result list) even though the user cannot access the contents of the record or folder.

## Protective marking scheme

### *Minimum requirements*

- B.4.16. The ERMS must support a protective marking scheme in order to control which users are allowed access to which electronic records and electronic folders.
- B.4.17. The ERMS must enable, but not necessarily require, a protective marking<sup>13</sup>, that is made up of one or more sub-markings, to be allocated to each electronic record and electronic folder, and to each user of the system.
- B.4.18. The ERMS must support a hierarchy of security ‘classification’<sup>14</sup> categories from unrestricted access at the lowest level to highly restricted access at the highest level; each level of this hierarchy represents a separate sub-marking.
- The ERMS must enable exactly one of these security category sub-markings to be applied to an electronic record or electronic folder as an element of metadata.
- B.4.19. The ERMS must enable each user to be allocated exactly one security category as defined in *B.4.18*, as an element of metadata.
- B.4.20. The ERMS must limit access to electronic records and electronic folders which have been allocated a security category to a user who have been assigned an equal or higher category, *unless* the item has been allocated further access control markings (including named user lists as in *B.4.10*) which that user has not also been equivalently allocated.
- B.4.21. The ERMS must support a default value of ‘Unclassified’ to an electronic record or folder not allocated any other access control marking.
- B.4.22. The ERMS must allow the addition of a descriptor<sup>15</sup> sub-marking to an electronic record or folder as an element of metadata; allocation of a descriptor will be used in conjunction with named user lists (*B.4.10*).
- B.4.23. Where full-text retrieval of record content is available, the ERMS must ensure that a user who is not allowed access to an electronic record or folder *cannot* receive any information about the record or folder as a result of a full-text search.

---

<sup>13</sup> Security classification categories are set out in the Reference Document at p.27-28.

<sup>14</sup> Note that the term ‘classification’ is used here to refer to categories of protective marking access control, and does not refer to the organisation of records in a corporate fileplan or thesaurus.

*Desirable requirements*

- B.4.24. The ERMS should support the addition of further types of sub-marking<sup>15</sup> to an electronic record or folder, and should support the allocation of more than one sub-marking in each type. Where further sub-markings are implemented, the ERMS must meet the requirements detailed in *B.4.28 – B.4.31*.
- B.4.25. The ERMS should be capable of preventing an electronic folder from having a lower security classification category than any electronic record within that folder.
- B.4.26. The ERMS should enable a systems administrator to define valid combinations of the sub-markings that are implemented.
- B.4.27. The ERMS should require that an electronic record or folder bearing a descriptor must also be allocated a list of named users, to which access is limited.

**Further protective sub-marking requirements**

- B.4.28. The ERMS may support the use of the following sub-marking types:
- *codewords*
  - *caveats*
  - *IDO markings*.

*Minimum requirements*

- B.4.29. The ERMS must enable a systems administrator to maintain the list of valid terms<sup>15</sup> (single words or phrases) for each sub-marking type implemented.
- B.4.30. Where a *codeword* sub-marking is implemented, the ERMS must allow the systems administrator to maintain a list of users allowed to access electronic records or folders to which that codeword has been allocated; and must limit access to such records or folders to users in this list.
- B.4.31. Where a *caveat* and/or *IDO marking* type is implemented, the ERMS must allow each user to be assigned:
- either several nationalities, if the ERMS is able to relate individual nationalities to caveats and/or IDO markings
  - or an unlimited number of caveats and/or IDO markings
- and must limit access to electronic records or folders bearing a caveat and/or IDO marking to users who have been assigned appropriate nationality(ies) and/or caveat(s).

---

<sup>15</sup> Descriptors and further types of protective sub-marking, and example terms in use for each of these types, are detailed in the Reference Document at p.27-28.

## Control of access to system functions and facilities

### *Minimum requirements*

- B.4.32. The ERMS must enable a systems administrator to define a set of user rôles, and to assign specific functions or groups of functions to each user rôle.
- B.4.33. The ERMS must ensure that all users are allocated to one or more user rôle(s).
- B.4.34. The ERMS must be able to limit access to system functions and facilities, so that all users will only be able to carry out functions which are assigned to the user rôle(s) of which they are member(s).

### *Desirable requirements*

- B.4.35. The ERMS should be capable of removing the visibility of functions from users who do not have access to those functions in their allocated user rôle.
- B.4.36. The ERMS should support a model of user rôles which enables functions to be allocated to the rôles as set out in the supporting Reference Document<sup>16</sup>.

---

<sup>16</sup> User rôles are set out in the reference Document at p.32-34.

## 5 : Audit and authentication

### High level requirements

- The ERMS must be capable of management and control of electronic records to the standards necessary for compliance with requirements for legal admissibility, and be capable of demonstrating this compliance.
- The ERMS must keep an unalterable audit trail capable of recording all the actions that are taken upon an electronic record, electronic folder or filing structure; the user initiating the action; and the date and time of the event.
- The ERMS must be able to maintain audit trails for the life of the electronic record and electronic folder, and be able to export audit trails for electronic records and electronic folders.
- The ERMS must be capable of storing details of the successful verification of a digitally signed record as metadata with the electronic record itself, and should be capable of storing the electronic signatures and verifying information if necessary.

### Detailed requirements

#### Audit

##### *Minimum requirements*

- B.5.1. The ERMS must be able to record an audit trail of events within the system, that records:
- the function which is being applied
  - the object(s) to which the function is being applied
  - the user applying the function
  - the date and time of application
- where events occur to:
- groups of electronic folders
  - individual electronic folders
  - electronic parts
  - electronic records
  - metadata associated with any of the above.
- B.5.2. The ERMS must track and record events automatically without manual intervention, once the audit trail facility has been activated.
- B.5.3. The ERMS must ensure that audit trail data cannot be modified in any way or deleted by any user.

- B.5.4. The ERMS must maintain the audit trail for as long as required, which will be at least for the life of the electronic record or electronic folder to which it refers.
- B.5.5. 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.
- B.5.6. The ERMS must be able to export audit trails for electronic records, electronic folders and groups of folders.
- B.5.7. The ERMS must be able to record violations, and attempted violations, of access control mechanisms.
- B.5.8. In particular, the ERMS must be capable of recording in the audit trail the following information:
- the date and time of declaration of all electronic records
  - the initial, and any subsequent, entry(ies) of an electronic record within the electronic fileplan
  - re-location of an electronic record to another electronic folder
  - re-location of an electronic folder within the electronic fileplan
  - re-allocation of a disposal schedule to an electronic folder
  - the occurrence of a change made to any metadata associated with electronic folders or electronic records
  - date and time of creation, amendment and deletion of indexes
  - changes made to the allocation of access control markings to an electronic folder, electronic record or user
  - export or transfer actions carried out on an electronic folder
  - deletion / destruction actions on an electronic folder or electronic record.

*Desirable requirements*

- B.5.9. The ERMS should be capable of registering the destruction of electronic records, electronic folders and groups of folders in an audit trail for *permanent preservation*.
- B.5.10. The ERMS should allow the extent of audit trail tracking and recording to be user-configurable, so that a systems administrator can select the functions which are automatically recorded; the ERMS must then ensure that this selection itself is recorded and that all changes are recorded.
- B.5.11. The ERMS should be capable of recording all possible events in the audit trail.
- B.5.12. The ERMS should be capable of recording the data changes made during any recorded event in the audit trail.

## Electronic signatures, digital signatures and encryption

### *Minimum requirements*

- B.5.13. The ERMS must be able to retain the information that an electronic signature has been verified as authentic, as a metadata element bound to the electronic record with which the signature is associated.
- B.5.14. The ERMS must be able to retain and preserve as metadata, details about the process of verification for a digital signature, including:
- the Certification Authority with which the signature has been validated
  - any checks made against a certification revocation list or similar status verification agency.
- B.5.15. 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 marking allocated to that record.
- B.5.16. Where an electronic record has been transmitted in encrypted form by a software application which interfaces with the ERMS, the ERMS must be able to keep as metadata with that record:
- the fact of encrypted transmission
  - the type of algorithm
  - the level of encryption used.

### *Desirable requirements*

- B.5.17. The ERMS should be able to preserve with the electronic record:
- the digital signature associated with that record
  - the digital certificate 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.
- B.5.18. The ERMS should be capable of checking the validity of a digital signature at the time of declaration of the record.
- B.5.19. The ERMS should be capable of checking the validity of a digital signature after a record has been declared, and where it has this capability the ERMS must be capable of including within the audit trail:
- the fact that the validity of the signature was checked
  - the fact that the validity of the associated certificate was checked
  - the date and time that the checking occurred.

- B.5.20. The ERMS should be able to ensure the capture of, and declare, an encrypted record directly from a software application which has an encrypting capability, and restrict access to those users listed as holding the relevant decryption key.

## 6 : Hybrid folder management

### High level requirements

- The ERMS must be able to declare, and classify to one or more electronic folders within the fileplan, markers (metadata) for paper and other records arising from the course of business.
- The ERMS must support the integration of information about paper folders (physically held outside the system) within the electronic fileplan, and support the use of access control and disposal schedules for these paper folders.
- The ERMS must support the management of hybrid folders, which have both a paper and an electronic existence, sharing substantively the same identifying metadata (such as title and numerical reference code); and must maintain a close link between the two related folders.
- The ERMS must be able to search for and retrieve paper folders and markers by means of paper folder and marker metadata.
- The ERMS should support tracking of paper folders by the provision of check-out, check-in and bring forward facilities which record the current location of the folder.

### Detailed requirements

#### *Minimum requirements*

- B.6.1. The ERMS must be able to declare markers – that is, a metadata profile of a record that is not physically held within the ERMS, often but not necessarily limited to a paper record.
- B.6.2. The ERMS must allow the definition of a metadata element set for markers separately from the metadata element set for electronic records; marker metadata must include information about the physical location of the marker.
- B.6.3. The ERMS must support the ability to define different marker types, with different metadata elements sets for each type. Examples of marker types are:
  - information about a paper record
  - information about a database
  - information about a video.
- B.6.4. The ERMS must be able to associate a marker with one or more electronic folders.
- B.6.5. The ERMS must be able to retrieve and display a marker when the electronic folder with which it is associated is retrieved.
- B.6.6. The ERMS must support the ability to enter (a metadata profile of) a paper folder in the electronic fileplan; a paper folder may contain metadata profiling

one or more paper parts. A paper part will not contain electronic records, and will not contain markers.

- B.6.7. The ERMS must allow a different metadata element set to be configured for paper folders than that for electronic folders; paper folder metadata must include information on the physical location of the paper folder.
- B.6.8. The ERMS must allow the creation of hybrid folders – a paper folder which is associated as a hybrid with an electronic folder – and allow use of the same folder title or numerical reference code, but with an added indication that it is a hybrid paper folder.
- B.6.9. The ERMS must allow the creation of a paper folder which is *not* associated with an electronic record as a hybrid folder.
- B.6.10. The ERMS must be able to allocate a protective marking, and/or a named list of users, to all markers and paper folders and must be able to control user access to markers and paper folders consistent with access controls for electronic records and folders.
- B.6.11. The ERMS must be able to search for and retrieve markers and all paper folders by metadata elements.
- B.6.12. The ERMS must ensure that retrieval of a complete electronic folder also retrieves all markers associated with that folder.
- B.6.13. The ERMS must ensure that retrieval of a hybrid electronic folder also retrieves any associated hybrid paper folder.
- B.6.14. The ERMS must ensure that a hybrid paper folder is allocated the same protective marking as an associated hybrid electronic folder.
- B.6.15. The ERMS must support the application of the same disposal schedule to the hybrid paper folder that is allocated to an associated hybrid electronic folder.
- B.6.16. The ERMS must be able to apply any review decision made on a hybrid electronic folder to a hybrid paper folder with which it is associated.
- B.6.17. The ERMS must be able to alert the records administrator to the existence and location of any hybrid paper folder associated with a hybrid electronic folder which is to be exported or transferred.
- B.6.18. The ERMS must be able to record changes made to the metadata of markers and all paper folders in the audit trail.

*Desirable requirements*

- B.6.19. The ERMS should support the allocation of a disposal schedule to every paper folder in the electronic fileplan, that will function consistently with scheduling for electronic folders, notifying the records administrator when the disposal schedule comes into force.

## SECTION B : ADDITIONAL REQUIREMENTS

---

- B.6.20. The ERMS should support the application of a review decision taken on a group of folders to any paper folders within that group, by notifying the records administrator of necessary actions to be taken on the paper folders.
- B.6.21. The ERMS should support the application of a review decision taken on an electronic folder with any markers within that folder, by notifying the records administrator of necessary actions to be taken on the markers.
- B.6.22. The ERMS should be able to export and transfer markers and paper folder metadata.
- B.6.23. The ERMS should support a paper folder metadata element set which enables the tracking of physical paper folders, including elements for:
- physical location
  - barcode
  - check-out to a user
  - check-in from a user
  - bring forward date.
- B.6.24. The ERMS should be capable of offering check-out and check-in facilities for paper folders profiled in the system, in particular enabling the ability to record a specific user or location to which a physical paper folder is checked-out, and to display this information if the paper folder is retrieved in the ERMS by another user.
- B.6.25. The ERMS should be capable of offering a bring forward facility for paper folders profiled in the system, enabling a user to enter a bring forward or reserve date for a physical paper folder, and generating a consequent message for transmission to the current holder of that folder or the record manager, according to configuration.



## **Section C : Supporting system requirements**

### **Rationale**

This section sets out features which some departments and agencies will require and others will not; for example, advanced search and retrieval facilities are likely to be required by a policy-based department, while a smaller or casework-based department may not need this level of sophistication. The requirements for these modules are given at a lesser level of specificity than those in earlier sections, since they are already reasonably well understood application areas in their own right.

#### *Document management facilities*

Some organizations will require document management facilities as part of a fully integrated electronic document and records management system. An electronic records management system may provide these facilities directly itself or integrate with another software package which does so; and this may already be in use in the organization. While there are many wider aspects of document management not covered here, an electronic records management system will require access to facilities for document and metadata capture, and will need to be capable of managing electronic documents and document versions alongside electronic records.

#### *Advanced search and retrieval*

Some organisations will require more advanced search and retrieval facilities than those mandated in Section A. For these organisations, it may be necessary to retrieve electronic records by content and to employ more sophisticated searching mechanisms to do so, including the use of a standard thesaurus.

#### *Bulk import*

It may be necessary to reliably import electronic records, file structures and metadata from document management applications, and electronic documents from operating system directories and other sources in order to declare and manage them as records.

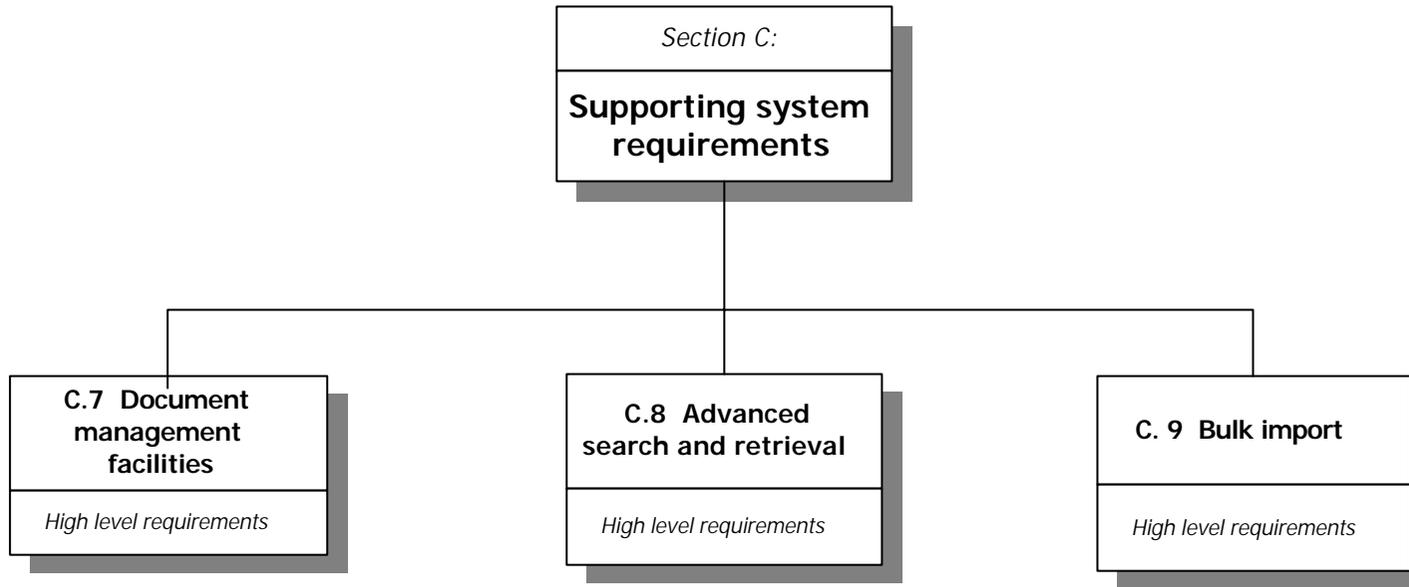


Fig. 4 : Structure of Section C

## 7 : Document management facilities

### High level requirements

- The ERMS with document management facilities must be able to capture electronic documents arising in the course of business and pass them to the process for declaration as electronic records:
  - directly on creation from an office application package, or other record-creating system
  - by acquisition of an existing electronic document, for example: an electronic document produced by scanning of a paper document; an electronic document held in an operating system user directory

and be capable of adding an interface to new office applications as these are brought into use by the organisation.

- The ERMS with document management facilities must be able to:
  - capture and declare an electronic record in one process
  - capture an electronic document and declare it to be an electronic record at a later date.
- The ERMS with document management facilities must be able to acquire metadata elements directly from the record-generating application, and allow additional metadata elements to be completed by the user.
- The ERMS with document management facilities must be able to manage electronic documents (which have not been declared as records) within the same electronic fileplan and access control mechanisms as electronic records.
- The ERMS with document management facilities must be capable of allowing an electronic document that *has not* been declared as a record to be edited, while preventing an electronic document that *has* been declared as a record from being edited.
- The ERMS with document management facilities must be capable of managing versions of an electronic document, as separate but related entities, while maintaining the link between them.
- 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.

## 8 : Advanced search and retrieval

### High level requirements

- The ERMS must allow a systems administrator to specify any element of record and folder metadata, and optionally full record content, that is to be indexed for future retrieval, and to define stop lists; and must support the ability to change this configuration at a later date.
- The ERMS must be able to retrieve electronic records and electronic folders by an integrated search mechanism on both record content, and record and folder metadata.
- The ERMS must provide search mechanisms which offer both a browsing or graphical navigation approach within the folder structure, and a direct searching approach.
- The ERMS must provide Boolean and probability-based full-text search and retrieval mechanisms, and relevance ranking of retrieval results.
- The ERMS must provide user assistance by query formulation, including the use of a controlled vocabulary system.
- The ERMS must support the sorting, printing and saving of search results in variable display formats.
- Where (non-record) electronic documents are managed alongside electronic records in the same system, the ERMS must be able to search for and retrieve both documents and records in an integrated manner.
- The ERMS must ensure that all retrieval operations are consistent with all access control restrictions, so that an unauthorised user cannot access folders or records by use of an advanced search and retrieval mechanism.
- The ERMS should allow search requests to be made from outside the system, and support the ability to exchange search requests and search results with other ERM systems.

## 9 : Bulk import

### High level requirements

- The ERMS must be able to import in bulk:
  - electronic records and associated metadata
  - a pre-existing folder structure
  - entries of electronic records in that folder structurewithout degradation of content or format, and without loss of any element of the record, including linkages, attachments and embedded objects.
  
- The ERMS must be able to carry out bulk import operations on groups of existing electronic documents (not already held in a records management system), including:
  - the ability to import electronic documents and declare as records
  - the ability to import any existing metadata with such documents, and map this to the metadata element set in the ERMS
  - the ability to import any existing folder structure with such documents.



## **Section D : Informative additional requirements**

### **Rationale**

Not all the attributes of a successful system can be defined in terms of functionality. In practice, other attributes – *non-functional* requirements – are important to success. While they often are difficult to define and measure objectively, it is nevertheless valuable to identify them so that they can be considered, if only (in some cases) in subjective terms.

In addition, departments will need to consider their needs in relation to current implemented technical and operational standards, and in relation to customer support services including documentation, training and consultancy.

Organisations will need to add their own specific requirements in these areas, depending on their organisational size and structure, physical characteristics and current technical operating environment. This section is intended as a checklist of aspects which departments will need to consider when developing their own specific requirements, to be added to the generic requirements given in earlier sections. This checklist may be of particular use to those within the smaller department or agency charged with developing a specification for electronic records management.

### **D.10 : Non-functional requirements**

Departments and agencies should consider their requirements, in the light of their individual context, for the following non-functional areas:

#### **D.10.1 Ease of use**

Departments and agencies should consider the extent to which the ERMS is easy to use, for all kinds of user for whom it is intended, and with minimal training, including the following aspects:

- The provision of online help throughout the ERMS, and the extent of any context-sensitive online help facility.
- The extent to which all error message are meaningful, and can be appropriately acted upon, by the users who are likely to see them.
- The application of a single, or a small number, of user interface rules; and their consistency with the operating system environment in which the ERMS operates.
- ERMS provision of end user and administrator functions which are easy to use and intuitive throughout (as may be assessed by a panel of typical users).
- The suitability of the user interface for users with disabilities; that is, compatibility with specialist software that may be used, with appropriate interface guidelines.
- The ability of users to move, re-size and modify the appearance of display windows, to select sound and volume of audio alerts, and to save modifications in a user profile.

- The provision of persistent, user-definable defaults for data entry where desirable.

### D.10.2 Performance and scalability

Departments and agencies 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, including:

- The ability with which the ERMS provides 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.

- The ability to perform a simple search within 3 seconds and a complex search (combining four terms) within 10 seconds.
- The ability to retrieve and display the first page of a record which *has* been accessed within the previous three months within 4 seconds.
- The ability to retrieve and display the first page of a record which *has not* been accessed within the previous three months within 20 seconds.
- The ability to allow a single implementation of the system to have an electronic record store of at least <xxx><sup>17</sup> Terabytes or <xxx thousand/million> records, and to serve at least <xx hundred/thousand> users simultaneously.
- The ability to allow a system implementation to be expanded, in a controlled manner, up at least <xx hundred /thousand> users while providing effective continuity of service.
- The ability to support the above without imposing undue systems/account management overheads.
- The absence of any features which would preclude use in small or large organisations, with equally variable numbers of differently-sized organisational units.

### D.10.3 Maintainability

Departments and agencies should consider the extent to which the ERMS includes features which allow its administrators to maintain it, including:

- The ability to make bulk changes in record organisation and folder structure and to indexing information, and to ensure all metadata and audit trail data are

---

<sup>17</sup> Estimates of record and user population to be inserted by the department or agency according to size and scale of operations.

handled correctly, in order to make the following kinds of organisational change<sup>18</sup>:

- 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 (or more) organisations.
- The ability to support the fluid movement of users between organisational units, individually or in bulk.
  - The ability to retrieve, display and re-configure systems parameters and choices made at implementation – for example, on elements to be indexed – and to re-allocate users to user rôles, and functions to user rôles, in a controlled manner and without undue effort.
  - The ability to provide back-up facilities, and to rebuild forward using back-up and audit trails.
  - The ability to provide recovery and rollback facilities in the case of system failure or update error, and to notify administrators of the results.
  - The ability to monitor available storage space, and provide notification to administrators when necessary.
  - The extent of commitment to ongoing development and support, so that the organisation can be confident of upgrade as a result of developments in systems and application software.

---

<sup>18</sup> Note: In the following, changes to organisational units imply corresponding changes to the fileplans of the units and their user populations.

## D. 11 : Technical standards

The ERMS should comply with relevant *de facto* and *de jure* standards and existing technology; where possible, it is desirable that the ERMS should make use of open rather than proprietary specifications and formats. Departments and agencies may need to consider their requirements, in the light of their individual context, in the following areas of standards:

### D.11.1 Hardware, operating systems and network environments

- Hardware environment: client-server platforms, workstation environments.
- Operating system environment: e.g. Microsoft Windows (NT4, 95,98), MacOS, Unix version.
- User interface industry standards: Microsoft Windows, Macintosh, X-Windows.
- Optional (Intranet) browser interface.
- Network protocols and operating system: TCP/IP, Ethernet type, Novell, Windows NT Server, etc.

### D.11.2 Supporting software

- Any database management system license/implementation necessary for integration the ERMS, including the SQL language version.
- The range of user applications (word processors, spreadsheets, e-mail systems, and any other applications) which the ERMS will be required to interface with for the capture of electronic records.
- The range of output formats which the ERMS will be required to produce for individual or bulk exports, including PRO-required formats for permanent preservation, and electronic publishing formats such as HTML 4.0 and XML.
- Search and retrieval and information exchange standards, including Z39.50.
- TWAIN and/or Isis scanner interfaces and Group IV facsimile compression.
- TIFF v6 image format, and if colour images are supported, JPEG, PNG, GIF or other user-selectable format.

### D.11.3 Other standards

- Compliance with BSI DISC PD0008:1999 *Code of practice on legal admissibility and evidential weight of information stored electronically*.
- Compliance with BSI DISC PD2000-1:1998 *A definition of Year 2000 conformity requirements* for the use of 20<sup>th</sup> century dates<sup>19</sup>.

---

<sup>19</sup> Use of 20<sup>th</sup> century dates may be required on and after the calendar year 2000 for inactive and archival material.

## SECTION D : INFORMATIVE SYSTEM REQUIREMENTS

---

- If a thesaurus is implemented, compliance with the ISO 2788 standard *Guidelines for the establishment and development of monolingual thesauri*, ISO 2788 – 1986.
- Certification to US DoD 5051.2-STD *Design criteria standard for electronic records management software applications*.

## D.12 Documentation, consultancy and training

Departments and agencies should consider their requirements, in the light of their individual context, for the following areas:

### D.12.1 Documentation and training

- The completeness of the documentation set which is delivered with the ERMS, and the frequency and completeness of update to this documentation, allowing the user organisation to:
  - continue to use and maintain the system should the supplier cease support
  - export all information and metadata from the system, on migration to a new system, or transfer of records to another organisation.
- The support which the supplier can offer in training users and administrators in use of the system, including:
  - training in system implementation and maintenance for systems administrators
  - training in systems management for records managers and records administrators
  - training materials for use with end users, as part of the implementation process.
- Help desk and user enquiry facilities.

### D.12.2 Supplier consultancy services

- The consultancy support which the supplier can offer for:
  - implementation-specific customisation of the ERMS for specific organisational requirements, including interfacing with document-generating applications
  - system configuration at time of implementation and re-configuration at a later time
  - planned maintenance and unanticipated problem resolution; and the speed of response to unexpected problems.