UNITED NATIONS
Department of Management
Archives and Records Management Section

Standard

April 2003

Functional Requirements for Record-keeping Systems in the United Nations Secretariat

Approved by: Bridget Sisk
Approval date: 2003
Contact: sisk@un.org
Review date:

Standard

Functional Requirements for Record-keeping Systems

Contents:

ANNEXES
None

Introduction

What are functional requirements?

Functional requirements are a set of generic functional requirements that are necessary, or highly desirable set of requirements for a credible record-keeping system. They are particularly useful for the development of record-keeping systems for managing electronic records. The requirements are organized under the broad functional headings of Record Classification; Record Capture, Creation and Management; Search, Display and Presentation; Retention and Disposal; Access Control; Audit; Reporting; Usability; Design and Performance; Compliance with other standards. In addition, the requirements are graded as either mandatory or various levels of desirability (see below).

Purpose of this document

The draft functional requirements have been produced as a comprehensive set of functional requirements for use in the development of record-keeping systems. They incorporate:

- United Nations work in determining requirements for electronic records management in United Nations offices;
- experience in testing software applications, and
- lessons shared by international experience.

This Statement of Functional Requirements supersedes previous electronic record-keeping functional advice issued by the United Nations Archives and Records Management Section (ARMS).

This is a Statement of generic requirements and not a full specification.

These requirements form a baseline that sets out the minimum necessary for a credible electronic records management system. United Nations offices wishing to make use of these requirements, as a baseline or benchmark, will always need to consider their own specific business needs and context in determining their own statement of functional requirements. These generic requirements must be tailored by:

- adding specialist business 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 *highly desirable* are *mandatory* for their own context;

- assessing whether any requirements listed here as *desirable* are *highly desirable* for their own context.

Audience

The Functional Requirements are to be used as a reference tool by records managers, information managers, and information technology managers in the United Nations, as well as the software vendor/integrator community.

Level of requirement

This Statement introduces a *Highly Desirable* level of requirement for UN offices. Many of these highly desirable requirements set out facilities needed for effective records management in relation to protecting sensitive data and ensuring information remains accessible for as long as it is required to be kept.

Some United Nations offices may consider these requirements as mandatory now, and many more are likely to do so with the increased awareness of the importance of electronic record-keeping. The highly desirable category provides a transition space for Record-keeping Systems (RKS) product suppliers to move towards incorporation of these features within established product development cycles.

In this document:

- mandatory requirements are indicated by the phrase “The Record-keeping System must...”

- highly desirable requirements are indicated by the phrase “The Record-keeping System should...”

- desirable requirements are indicated by the phrase “The Record-keeping System may ...”.

Each numbered requirement is labelled as:

(M) = Mandatory = “The Record-keeping System must ...”

(HD) = Highly Desirable = “The Record-keeping System should ...”

(D) = Desirable = “The Record-keeping System may ..”

MUST - This word means that the numbered requirement as defined is an absolute requirement.

MUST NOT -This phrase means that the numbered requirement as defined is an absolute prohibition.

SHOULD - This word means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course. An implementation which does not include such an item MUST be prepared to interoperate with another implementation which does include the item, though perhaps with reduced functionality. An implementation which does include a particular item MUST be prepared to interoperate with another implementation which does not include the item (except of course for the feature which the item provides).

MAY - This word means that the numbered requirement is optional. One vendor may choose to include the requirement because a particular marketplace requires it or because the vendor feels that it enhances the product, while another vendor may omit the requirement. An implementation which does not include such an option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. An implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except of course for the feature which the option provides).

WHERE - Where a SHOULD option is taken, subsequent requirements may use the phrase "Where < a feature is provided>, the RKS must ...". Here, MUST means that if the highly desirable or desirable option is offered, the mandatory rider is an absolute requirement. If the highly desirable or desirable option is not offered, the rider does not apply.

In section 9, the label (A) is sometimes used in conjunction with (M) and (HD) and (D). This indicates that the requirement is Advisory, and relates to the use of this requirement in the normal testing process, where stress loads and response measures cannot easily be replicated. It is, however, Advisory for departments and agencies to include equivalent considerations as Mandatory, or Highly Desirable, within their own specific Statement of Requirements. More discussion on the use of these requirements for departmental/office projects, is contained in volume *3: Implementation Guidelines.*

Structure of functional requirements
This document is divided into two main sections:

Section A: sets out the core requirements for a Record-keeping System, in ten sub-sections.

Section B: lists a developing set of optional modules for additional features which may be incorporated with an RKS. Where a module is offered by a product, mandatory requirements apply. If a module is not offered by a product, requirements do not come into play at all. Optional modules do not attempt to define the entire area of each option; rather, only those features which overlap with, or will have an impact on, requirements for management of electronic records.

Section A: sets out the core requirements for an electronic records management system in some detail. The main areas cover the ability to:

- build and maintain a classification scheme, against which folders are classified;
- manage folders, parts and records, and their metadata;

- create an electronic document as a corporate record, and to maintain its integrity as an authentic representation of a business action or decision;

- search for and retrieve records;

- consistently manage the retention and disposition of whole folders and records, retaining what should be kept and disposing of what should not, whether by transfer to another organisation or destruction;

- control access to folders and records, and to maintain an auditable track of actions taken on them;

- provide manageable, usable and robust mechanisms to carry out core functions.

Electronic records will need to be organised into cognate groups for access and retrieval, management and eventual disposal, in which a complete group of records which relate to the same business activity, case or theme is maintained, 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.

Records on a specific topic are grouped together into folders, which are allocated to a class. Classes are arranged, usually in a hierarchical structure, to reflect and support the business activities of an organisation. Specific scheduling and management characteristics will be attached to every individual folder (sometimes inherited by virtue of the class to which they belong), according to the record-keeping requirements of the business process which they represent.

Electronic documents will be created 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 created, 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.

Once created as a corporate record, the content of the record (and some of the metadata) must not be capable of being changed – or it would no longer be a reliable and authentic record.

Every electronic record will be allocated to a folder at the time of creation, and will be controlled by the records 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 only exception to whole-folder management of records applies to records created as a specific type which allows a different behaviour; this will be needed to manage aspects of privacy and personal data.

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.

In the near future it may be necessary to export (transfer) some folders of records to the United Nations Archives or other appointed place of deposit for permanent preservation; and it may be necessary to export folders to another RKS. Transfer will include both *record content* and descriptive material relating to *record context*, such as file structure, folder and record metadata. All records will need, at some point, to be destroyed within the system, so that they cannot be restored. Information and audit trails will need to record such actions.

Throughout the life of the record, various forms of access control may need to be applied, to ensure continued integrity and to protect the contents from inappropriate use. Auditing of all actions taken on a record is necessary to demonstrate such integrity and ensure accountability and legal admissibility as necessary.

Section B: sets out additional features closely related to electronic records management, which some products but not others may offer.

Authentication and encryption facilities enable integration with standard digital signature and certification technologies, particularly where this is related to transactional records received in this way.

Document management facilities enable an integrated document and records management system to be offered, so that the whole document and record lifecycle can be managed, from the creation, drafting and formalisation of documents to the creation, management and disposal of records.

Hybrid and Physical folder management enables legacy paper records to be managed alongside electronic records; and for an integrated approach to continuing paper records in the form of hybrid folders.

Other optional modules in Section B are planned. These are likely to cover:

Content management and EKM;

Casework and workflow;

Image management and document scanning;

Preparing records for transfer.

Acknowledgements

This draft of the Functional Requirements was adapted from: *Requirements for Electronic Records Management Systems, 1: Functional Requirements,2002 Revision: Final Version, Public Record Office, The National Archives, Kew, United Kingdom*.

The United Nations Archives and Records Management Section is grateful to the Public Record Office for permission to adapt their work.

Section A: Core requirements

A .1: RECORD ORGANISATION

Classification scheme and record plan

A.1.1 (M) The RKS must support representation of a business classification scheme, by which electronic folders are placed in an organised structure, consistent with the nature of the classification scheme; the classification scheme and the folders which are classified against this scheme together make up the record plan.

A.1.2 (M) The RKS must be capable of supporting a hierarchical (minimum requirement) business classification scheme[1] with a minimum of three levels below the root level; and must support the use of varying numbers (some 2, some 3) of levels at different points in the classification scheme[2].

A.1.3 (M) The RKS must support the initial construction of a business classification scheme within the RMS, in preparation for the creation of folders and before the receipt of electronic records.

A.1.4 (M) The RKS must allow an authorised user to add new classes to the classification scheme, except where folders have already been created under an existing class; in which case, the RKS must be capable of preventing the addition of new descendant classes to that existing class.

A.1.5 (M) The RKS must not, by its own architecture or design, impose any practical limit on the number of classes that can be created at any point within the classification scheme, or within the entire RKS[3].

A.1.6 (M) The RKS must enable a whole class, including all classes, folders, parts, and records which fall under that class, to be relocated to another point in the classification scheme, retaining a history of their status prior to re-classification in metadata elements.

A.1.7 (HD) The RKS should enable an authorised user to mark an empty class as inactive and prevent any new folders being allocated to that class and its descendant classes.

A.1.8 (HD) The RKS should allow an Administrator to delete an empty class.

A.1.9 (M) Where the RKS allows deletion of a class, it must prevent deletion of a class that is not empty, until such time as all folders in that class, and its descendant classes, have been

---

[1] Note that the RKS may support the use of other types of structure; a hierarchical structure is the minimum requirement

[2] For example, some parts of scheme may use two levels, others may use three levels.

[3] A limit may be imposed by the underlying database technology which is used in a specific implementation

disposed of, and all minimum metadata retained following destruction of folders has been deleted.

A.1.10 (HD) The RKS should support multiple classification schemes._

A.1.11 (D) The RKS may support a distributed classification scheme which can be maintained across a network of electronic record repositories.

Class metadata

A.1.12 (M) The RKS must support the use of metadata for classes, and must restrict the ability to add or amend class metadata to an authorised user.

A.1.13 (M) The RKS must support the capture[4] and presentation[5] of metadata for classes as set out in the accompanying records management metadata standard.

A.1.14 (M) The RKS must provide at least two naming capabilities for classes (which will be used for the naming of folders):

- the capability to allocate a textual name to each class so that the accumulation of labels in any hierarchical path through the scheme are used to construct the full text name of that class;

- the capability to allocate a structured numeric or alphanumeric reference to each class, the accumulation of which codes in any hierarchical path through the scheme are used to construct the full file plan identifier[6] for that class where the text name and code are equivalent in meaning and mirror the semantic structure of the classification scheme.

A.1.15 (M) The RKS must allow both naming capabilities to be applied separately or together in the same application at the same time.

A.1.16 (M) The RKS must allow the pattern of naming[7] used by the naming capabilities to be configured by an Administrator.

---

[4] *Capture at time of creation or later editing*

[5] *Presentation for purposes of search and display, publication or export*

[6] *i.e. a file reference number*

[7] *For example, an example of the pattern XXX/YYYY-NNNN is CAB/2002-0029*

A.1.17 (M) The RKS must allow repetition, at different points in the classification scheme, of a class text name which represents only one segment of the class name.

A.1.18 (M) The RKS must ensure that the complete text name of each class (all segments of the name) is unique within the file plan.

A.1.19 (HD) The RKS should support a capability to import a structured assembly of classes and their metadata from an existing classification scheme or file plan in a bulk operation.

A.1.20 (M) The RKS must support the mandatory use of the complete text name of a class (i.e. all segments of the class name) as the primary element which, with the addition of an uncontrolled text element identifying the folder, will define the unique text name for a folder created under that class.

Example:
Regional planning : Public consultation : Correspondence
Regional planning : Public consultation : Exhibitions
where ***Correspondence*** *and* ***Exhibitions*** *are the text elements of the folder names, both falling under the same class* ***Regional planning: Public consultation****.*

A.1.21 (M) The RKS must support inheritance of metadata by lower levels of the classification scheme so that, by default, addition of a new class results in automatic inclusion of those attributes by the new class, which are defined as inherited from the higher level (i.e. inheritance on creation).

A.1.22 (HD) The RKS should support inheritance of metadata by lower levels of the classification scheme so that, by default, a *change* in the attributes of a class may be reflected in the inherited attributes of all classes descendent from that point in the scheme (retrospective inheritance).

A.1.23 (M) The RKS must support the ability to amend (i.e. over-ride) inherited metadata attributes on any individual class;

A.1.24 (HD) The RKS should support an optional class and folder naming mechanism that is based on controlled vocabulary terms and relationships and should support application of an ISO 2788 or ISO 5964 compliant thesaurus.

Folders

A.1.25 (M) Where a hierarchical classification scheme is in use, the RKS must allow the addition of folders to only the lowest level class in any single part of the scheme.

A.1.26 (HD) The RKS should support an optional class and folder structured naming mechanism which includes names (e.g. personal or corporate names) and dates (e.g. dates of birth) as elements of the class and folder name.

A.1.27 (HD) When creating a new electronic folder in a classification scheme which

uses a structured numerical or alphanumerical reference, the RKS should automatically generate the next sequential number available at that position within the scheme.

A.1.28 (M) The RKS must not, by its own architecture or design, impose any practical limit[8] on the number of folders which can be created under any class, or within the entire RKS.

Folder metadata

A.1.29 (M) The RKS must support the use of metadata for folders, and must be capable of restricting the addition or amendment of metadata elements to authorised users

A.1.30 (M) The RKS must support the capture and presentation of metadata for folders as set out in the accompanying records management metadata standard.

A.1.31 (M) The RKS must closely link folder metadata to the relevant RKS functionality which it represents (i.e. fulfil an active rather than merely descriptive purpose in achieving that functionality automatically).

A.1.32 (M) The RKS must support inheritance of metadata by folders allocated to a class so that, by default, addition of a *new* folder results in automatic inclusion of those attributes which derive from the class to which it is allocated[9] (i.e. inheritance on creation).

A.1.33 (HD) The RKS should support inheritance of metadata by folders allocated to a class so that a *change* in the attributes of a class can, optionally, be reflected in the inherited attributes of all folders already allocated to that class (retrospective inheritance).

A.1.34 (M) The RKS must support the ability to select a set of folders in order to perform the same amendment on the same metadata attribute on the whole selected set of folders in one process.

A.1.35 (M) The RKS must support the ability to amend (i.e. over-ride) inherited metadata attributes on any individual folder; where defined as being inherited by parts, such changes to a folder must be inherited by any and all parts into which that folder is segmented.

A.1.36 (M) The RKS must be capable of enforcing the *mandatory* use of the classification scheme to construct the folder name, as specified in *A.1.20*

A.1.37 (HD) The RKS should support the ability to optionally assign one or more controlled vocabulary terms by selection from a pre-defined list, to an electronic folder

A.1.38 (M) The RKS must support the use of user-defined metadata fields with folders, for recording descriptive information.

Folder management

---

[8] *Limit may be imposed by an underlying database but not by RKS*

[9] *See Reference Document for list of inherited elements*

A.1.39 (M) The RKS must enable recording of the opening date of a folder, which is a different attribute from, and may be chronologically earlier than, the physical creation date of the folder; this date to be actively used by disposal functionality. The opening date should automatically default to the creation date, but must be amendable by an authorised user.

Example: The ***open*** and ***close*** dates describe the time span of documents that are contained within a folder. A folder that is created on 23 August 2002, into which documents that have already been created over the previous twelve weeks are to be added, should have a folder open date of 1 June 2002. Otherwise, the time span of the folder would be incorrect.

A.1.40 (M) The RKS must be capable of configuration so that the ability to create new folders within an existing class can be controlled according to user role.

A.1.41 (M) The RKS must be able to close a folder and ensure that no new records or parts can be added to that closed folder, whilst leaving unchanged the ability to retrieve and view those records already added (but noting the requirement at *A.1.44*).

A.1.42 (M) The RKS must be able to restrict the ability to close a folder to an authorized user.

A.1.43 (M) The RKS must automatically record the closing date of the folder; this date to be actively used by disposal functionality.

A.1.44 (M) The RKS must allow an authorised user to open a previously closed folder for the addition of records and the creation of a new part if necessary; and subsequently to close that folder again; this action will not automatically change the closing date of the folder held as a metadata attribute.

A.1.45 (M) The RKS must ensure that a folder (which may be segmented into parts) can only contain electronic records (and markers representing physical records where used)[10].

A.1.46 (M) The RKS must prevent the destruction or deletion of an electronic folder and any of its records and metadata at all times, with the exceptions of:

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

A.1.47 (M) The RKS must allow an electronic folder or group of folders, and all parts and records which fall under that folder or folders, to be re-classified, by an authorised user, to a different point in the classification scheme, and should retain a history of their location prior to re-classification.

A.1.48 (M) The RKS must ensure that all electronic records and part(s) remain correctly allocated following the relocation of a folder or group of folders, so that all previous structural links between records, parts, and folders are retained.

---

[10] *i.e. a folder which contains records must not contain another folder as well: see requirements A.1.4 & A.1.2*

A.1.49 (HD) The RKS should allow all relevant folder and record metadata attributes which are determined by the point in the classification scheme (including those determined by inheritance) to be, optionally, automatically updated following the re-location of a folder.

A.1.50 (HD) The RKS should allow an authorised user to add the reasons for reclassification of a class, folder or record to the item(s) reclassified, once for all those re-classified in one operation.

A.1.51 (D) The RKS may support the creation of relational links (that is, 'see also' type links) between folders which are classified in different parts of the scheme or record plan.

Parts

A.1.52 (M) The RKS must support the concept of electronic parts, as a means to segment a folder for management purposes, making a clear distinction between the functionality of a folder and of a part[11].

A.1.53 (M) The RKS must support the use of metadata for parts.

A.1.54 (M) The RKS must support capture and presentation of metadata for parts as set out in the accompanying records management metadata standard.

A.1.55 (M) The RKS must closely link parts metadata to the relevant RKS functionality which it represents (i.e. fulfil an active rather than merely descriptive purpose in achieving that functionality automatically).

A.1.56 (M) The RKS must support implicit inheritance of metadata by parts of a folder, so that addition of a new part results in automatic inclusion of those folder attributes which determine behaviour of a part.

A.1.57 (M) The RKS must allow, but not necessarily require, the addition (opening) of new (i.e. second and subsequent) electronic parts to any electronic folder which is not closed; and should be able to restrict this capability to authorised users.

A.1.58 (M) The RKS must ensure that an electronic part will only contain electronic records (and markers representing physical records where used). It must not be possible for a part to contain another folder or part.

A.1.59 (M) The RKS must support the concept of open and closed electronic parts, and be capable of restricting the ability to close a part to authorised users.

A.1.60 (HD) The RKS should be able to automatically close a 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;

[11] *Where a folder contains only one part, the part may not be visible; any management action will take place at folder level. Parts must not be implemented as folders named "Part 1", "Part 2", etc*

- 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 and,
- optionally, to open a new part within that folder.

A.1.61 (M) The RKS must ensure that only the most recently created part within a folder will be open at any one time, and that all other parts within that folder will be closed, but noting the requirement at *A.1.67*,

A.1.62 (M) The RKS must ensure that the records contained in all parts, whether open or closed, are equally retrievable and viewable in the same search process.

A.1.63 (M) The RKS must prevent the addition of electronic records to a closed part, but noting the requirement at *A.1.67*.

A.1.64 (M) The RKS must automatically record the opening and closing dates of a part as metadata attributes.

A.1.65 (M) The RKS must ensure that the act of opening a new part automatically closes the preceding part.

A.1.66 (M) The RKS must automatically add new records classified against a folder to the currently open (the most recent) part, and should do so without requiring the user to explicitly choose a part[12] (but noting the exception at *A.1.67)*.

A.1.67 (M) The RKS must allow an authorised user to open a previously closed part for the addition of records, and subsequently to close that part again; this action will not, by default, change the closing date of the part held as metadata[13].

A.1.68 (M) The RKS must maintain full structural integrity of the class, folder, part and record structure at all times, regardless of maintenance activities, user actions, or component failures.

---

[12] *In many cases, there may be only ever one part to a folder – i.e. no second part is ever created – and in this case the part should not be visible. If a second part is created, the first should become visible.*

[13] *...and consequently affect the disposal date*

2: RECORD CAPTURE, CREATION AND MANAGEMENT

Capture

A.2.1 (M) The RKS must ensure that electronic documents can be captured, so that they can be created and stored as electronic records, from:

- standard office applications;
- operating system directory management facilities;
- e-mail client applications;
- images created by a document scanning system.

A.2.2 (M) The RKS must be capable of supporting document capture from new office applications, including open source software, as these are brought into use by an organisation.

A.2.3 (M) The RKS must provide an Application Programming Interface to enable integration with other business applications, so that records of transactions generated by operational and 'line-of-business' systems can be captured.

A.2.4 (M) The RKS must support the capture and creation of any electronic document which is stored as a single electronic file. Examples include:

- XML documents and forms
- word processing documents
- documents produced by text editors
- spreadsheets
- e-mail messages
- e-mail messages with attachments
- e-mail receipts
- encapsulated 'web pages', with all components, in a single physical file
- presentations
- desktop publishing documents
- PDF format documents
- document images from a scanning system
- single static images in common formats
- bit-mapped and vector graphics.

A.2.5 (HD) The RKS should be able to capture records which are composed of more than one component, retaining a closely bound relationship between all components, so that they are managed as a single record. Examples include:

- multimedia documents, including those with animation and video components;
- complete sessions from collaborative systems and 'chat rooms';
- webcasts;
- directly interlinked documents, for example by an OLE link;
- vector graphics and data in CAD/CAM systems; and
- map bases and data held in GIS systems.

A.2.6 (M) The RKS must allow users to capture, create and store electronic records in

their native format.

A.2.7 (M) The RKS must be able to capture an electronic document, even though the generating application is not present.

A.2.8 (M) Where the RKS captures records which are constructed of more than one component, it must be able to:

- capture and create the record in a way that retains the relationship between its constituent components;
- retain structural integrity of the record;
- support later integrated retrieval, display, management of the record as one unit; and
- dispose of the record as a whole unit, in one operation.

A.2.9 (M) The RKS must ensure the capture of, and be able to create, manage, display and dispose of an e-mail message with one or more attachments, maintaining e-mail text and attachments as a single electronic record.

A.2.10 (M) The RKS must be able to capture an e-mail message (and attachments if present) from within an e-mail client.

A.2.11 (M) The RKS must allow a user to choose whether to capture an e-mail message with attachment(s) as:

- the e-mail message only
- the e-mail message with attachments
- the attachment(s) only
- any sequence of all combinations[14] of the above

A.2.12 (HD) When capturing a document in its native format, the RKS should be capable of also capturing a rendition of that document in a standard format, and of storing native format and rendition in a close association. Standard rendition formats include: XML, PDF and Postscript.

Creation

A.2.13 (M) The RKS must support the process of creation, in which an electronic document is marked as a formal electronic record and is associated with one or more folders directly by an end user. (Capture and creation may take place in one operation)

A.2.14 (M) The RKS must prevent any amendment to the content of any electronic record (which has been created) by any user including an Administrator.

---

[14] *For example, to capture the e-mail plus attachment a one unit, and subsequently to capture the attachment separately*

A.2.15 (M) The RKS must at all times prevent the destruction or deletion of any electronic record (which has been created) with the exceptions of:

- destruction in accordance with a disposal schedule (A.4.67)
- deletion by a systems administrator as part of an audited procedure.(A.4.65)

A.2.16 (M) The RKS must support the naming of electronic records, and allow this name to be different from the existing electronic document filename (including e-mail subject lines used to construct record titles); if the existing filename is taken by default, the RKS must allow this name to be amended at the time of creation.

A.2.17 (M) The RKS must ensure that the content of the body of an e-mail message and the transmission details cannot be amended in any way between processes of capture and creation (but excluding the subject line used as record title, which can be edited).

A.2.18 (HD) The RKS should ensure that the content of and the transmission details of other electronic transactions with which the RKS is closely integrated cannot be amended in any way between processes of capture and creation.

A.2.19 (M) The RKS must ensure that all electronic records are assigned to at least one folders on completion of creation.

A.2.20 (M) The RKS must not impose, by its own architecture or design, any practical limit on the number of records which can be captured and created into a folder; or on the number of records which can be captured and created into the RKS as a whole.

A.2.21 (M) The RKS must allow an electronic record to be assigned to more than one Folder

A.2.22 (HD) The RKS should be capable of relating each assignment of the record, so that a later retrieval of one assignment enables identification and retrieval of all other assignments of that record made at the time of capture, or at a later stage from within the RKS[15].

A.2.23 (HD) The RKS should alert a user who is attempting to capture and create a document into a folder in which it has already been created, where this is evident from captured metadata.

A.2.24 (M) Where multiple assignments are achieved by use of a pointer system working with a single actual record, the RKS must be able to manage the integrity of all pointers or references, to ensure that:

- following a pointer, whichever folder that pointer is located in, will always result in correct retrieval of the record;

- change in location of a record also redirects any pointers which reference that record. at all times.

---

[15] *This requirement will not apply to records captured twice or more on separate occasion*

A.2.25 (HD) The RKS should provide support for decisions on the allocation of electronic records to electronic folders by:

- as initial default, showing only selected sections of the classification scheme, based on user or role profile
- suggesting the most recently used folders by that use r
- 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 suggesting folders by inferences drawn from the record contents.

Record types

A.2.26 (M) The RKS must support the definition of distinct record types[16], so that a different management policy can be applied to each record type.

A.2.27 (M) The RKS must support a default record type, which is available to all users with the ability to create new records.

A.2.28 (M) The RKS must support the definition of other record types by an Administrator, and must be capable of restricting the ability to create new records using these types to selected sets of end users.

A.2.29 (M) The RKS must enable defined record types to possess different metadata attributes, and to exhibit different behaviour based on these attributes, from the default record type; in particular, in relation to the allocation of disposal schedules.

Record metadata

A.2.30 (M) The RKS must support the use of metadata for electronic records

A.2.31 (M) The RKS must support the capture and presentation of metadata for electronic records as set out in the accompanying ARMS Standard on Record-keeping Metadata.

A.2.32 (M) The RKS must ensure the capture of all required metadata elements specified at systems configuration, and retain them with the electronic record in a tightly-bound relationship at all times.

A.2.33 (M) The RKS must be capable of automatically capturing:

- metadata acquired directly from an authoring application;
- metadata acquired directly from an operating system, and
- metadata generated by the RKS itself.

16 *Note that the term* record type *denotes a different concept from the term* template – *see glossary.*

A.2.34 (M) The RKS must be capable of capturing metadata acquired from the user at the time of creation.

A.2.35 (D) The RKS may provide an option for capturing metadata from the 'document properties' information held by a document where this is available; *but if so*, the RKS *must* allow this metadata to be edited[17] prior to creation.

A.2.36 (M) The RKS must support the ability to optionally assign one or more controlled vocabulary terms by selection from a pre-defined list to an electronic record.

A.2.37 (D) The RKS may support the ability to optionally assign one or more controlled vocabulary terms by selection from a ISO 2788 compliant thesaurus to an electronic record.

A.2.38 (M) The RKS must allow entry of further descriptive and other specified metadata at a later stage of processing (i.e. where this is allowable within other requirements); and must be able to restrict this ability to authorised users.

A.2.39 (M) The RKS must prevent any amendment of selected elements of metadata of the electronic record which have been acquired directly from the application package, the operating systems or the RKS itself (for example, certain dates) as defined by the ARMS metadata standard (but noting A.2.16 and A.2.38).

A.2.40 (M) The RKS must be capable of allowing a user to edit the content of selected elements of metadata of the electronic document during but not after the process of creation, including Title and Creator.

A.2.41 (M) The RKS must ensure that the content of selected items of metadata (a subset of those that may be changed) of the electronic record can only be changed by an authorised user[18] as defined by the ARMS metadata standard.

A.2.42 (M) The RKS must allow an authorised user, after creation, to edit the content of all metadata elements that have been captured from, or edited by, a user, but not those elements that have been system generated.

A.2.43 (M) The RKS must support:

- the definition of user-defined metadata elements for electronic records, by an Administrator;

- the required metadata element set for each new record type to be separately selected when defining the record type (within system requirements);

---

[17] *Because information in document properties may be unreliable.*

[18] *i.e. the RKS must be capable of controlling the metadata Edit function at the individual field level according to user role.*

- each selected metadata element to be defined as either mandatory or optional (except where the system requires metadata elements to be mandatory), and later reconfiguration of the selected metadata set.

A.2.44 (M) The RKS must record the date and time (to the nearest minute) of creation as a metadata element attached to the record; this data should in addition be recorded in the audit trail.

A.2.45 (M) The RKS must ensure the capture of e-mail transmission data and be capable of mapping this data to electronic record metadata elements, as set out in the ARMS Metadata Standard.

A.2.46 (M) When capturing an e-mail message, the RKS must ensure that e-mail transmission data is included in the body of the record, including sender, recipients, and date of receipt.

A.2.47 (M) The RKS must capture the '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, as well as the full version.

A.2.48 (M) The RKS must validate the content of selected metadata elements, to conform with requirements as set out in the accompanying metadata standard for electronic records management; in particular, in relation to date formats numeric and alphanumeric formats and in compliance with the UK Government Data Standards Catalogue

A.2.49 (M) The RKS must be able to allocate an identifier, unique within the system, to each electronic record on creation that serves to identify the record from the point of creation throughout the remainder of its life within the RKS.

Move, copy, extract and relate

A.2.50 (M) The RKS must allow an electronic record to be re-assigned to another electronic folder or part, and must be capable of restricting this ability to an authorised user.

A.2.51 (M) The RKS must be able to copy the contents of an existing electronic record, in order to create a new and separate electronic document, while ensuring the original record remains intact.

A.2.52 (HD) Where an RKS does not use pointers, the RKS should be able to make a controlled copy[19] of an existing electronic record, which can immediately be allocated to a different folder without change to the contents.

A.2.53 (M) When a record is retrieved, an RKS that is able to make controlled copies as in A.2.52 must make explicit the existence of, and offer an intuitively clear means of retrieving, any and all controlled copies made from that record.

---

[19] *For example, by use of an explicit Copy command from within the RKS*

A.2.54 (HD) The RKS should provide facilities for tracing all uncontrolled copies[20] made from an electronic record, that have been allocated to one or more different folders than the originating record.

A.2.55 (HD) The RKS should support the ability to create multiple entries for electronic records in different electronic folders without physical duplication of the electronic record itself.

A.2.56 (HD) The RKS should be able to allow the creation of an extract directly from an originating record, where portions of original content have been masked in the extract, while ensuring the original record remains intact.

A.2.57 (HD) The RKS should be able to create the extract as a record in its own right, but noting A.2.58.

A.2.58 (HD) The RKS should be able to automatically record the relationship between one or more extracts and the originating record.

A.2.59 (M) Where an RKS support direct creation of an extract it must be able to copy existing metadata attributes and access controls from the originating record to the extract, but allow selected items to be amended where necessary[21].

A.2.60 (HD) The RKS should allow the reason for the creation of an extract to be entered with the originating record.

A.2.61 (HD) When an originating record is retrieved, the RKS should make explicit the existence of, and offer an intuitively clear means of retrieving, all extracts made from that record.

A.2.62 (HD) The RKS should be able to mark a record as superseded, and create a navigable link to the superseding record.

Bulk import

A.2.63 (M) The RKS must be able to capture in bulk records exported from other records management and document management systems, including capture of:

- electronic records in their existing format, without degradation of content or structure, retaining the relationship between the components of any individual record;

- electronic records and all associated metadata, retaining the correct relationship between individual records and their metadata attributes, and

---

[20] *For example, taking a record out of the RKS as a copy, and subsequently adding as a new record creates an uncontrolled copy; facilities to trace the provenance of this copy if necessary will enable tracking of uncontrolled copies.*

[21] *For example, to allow the security category of the extract to be different from the category of the originating record.*

- the folder structure to which the records are assigned, and all associated metadata, retaining the correct relationship between records and folders.

A.2.64 (HD) The RKS should be to import any directly associated audit information with the record and/or folder, retaining this securely within the imported structure

A.2.65 (M) Within the schedule for implementation, the RKS must be able to directly import, in bulk, electronic records in their existing format with associated metadata that is presented according to a pre-defined schema[22] (schema to be defined based on the ARMS Metadata Standard), mapping this to the receiving RKS folder and metadata element structures.

A.2.66 (M) The RKS must be able to indirectly[23] import, in bulk, electronic records in their existing format with associated metadata that is presented in a non-standard format, mapping this to the receiving RKS folder and metadata element structures.

A.2.67 (HD) The RKS should be able to import, in bulk, existing electronic documents, in any and all supported formats, that have no associated metadata presented separately from the document, by:

- placing documents in queues for further processing
- automatically extracting metadata from the document properties where possible
- providing facilities for the addition of missing metadata, and the assignment of documents to folders
- supporting the creation of documents from these processing queues.

A.3: SEARCH, DISPLAY AND PRESENTATION

A.3.1 (M) The RKS must provide facilities for searching, retrieving and displaying classes folders, electronic records and markers (where markers are used).

A.3.2 (M) The RKS must provide an optional search and display interface via a web browser platform, to support retrieval and display of folders and records, and the subset of folder and record metadata normally available to the end user.

A.3.3 (M) The RKS must support graphical browsing of a classification scheme, and browsing directly from a class to the folders created under that class; and the direct selection, retrieval and display of electronic folders and their contents through this mechanism.

Searching

A.3.4 (M) The RKS must be capable of searching for all records management metadata

---

[22] *Schema is not yet developed*

.

[23] *Recognising that some intermediate processing is likely to be required since a non-standard format cannot be pre-defined.*

elements[24] including user-defined elements (noting requirement A.3.18)

A.3.5 (M) Where a controlled vocabulary or thesaurus is implemented, the RKS must be capable of searching for folders and records by terms from a controlled vocabulary or thesaurus.

A.3.6 (M) The RKS must be capable of searching the full-text content of electronic records.

A.3.7 (M) The RKS must present an integrated interface for searching both metadata and record content.

A.3.8 (M) The RKS must allow search terms to be qualified by specifying a metadata element, or record content, as source.

A.3.9 (M) The RKS must be capable of constructing searches by combining multiple terms, from multiple sources.

A.3.10 (M) The RKS must enable default search options for end users to be configured from the full range which is available.

A.3.11 (M) The RKS must provide facilities for defining and storing saved searches, for reuse by end users.

A.3.12 (HD) The RKS should support saved searches which can be run with varying parameters, including dates and date ranges.

A.3.13 (HD) The RKS should allow the use of propositional search logic, including:
- Boolean operators
- partial matches
- wildcard characters

A.3.14 (D) The RKS may allow the use of advanced search features, such as probabilistic retrieval, relevancy feedback, and pattern matching

A.3.15 (M) The RKS must present search results as a list of folders or records meeting search criteria; and must notify the user if the search results in a null set.

A.3.16 (M) The RKS must be able to search for and retrieve a complete electronic folder, and all its parts and records, and display a list of all, and only, those parts and records in the context of that folder as a discrete group and in a single retrieval process[25].

A.3.17 (M) The RKS must be able to search for, retrieve and list a set of electronic records taken from many different folders, by specifying values to be searched for in

[24] *As defined in accompanying ARMS Metadata Standard.*

[25] *That is, as a single set of operations, without need for the user to re-enter data already retrieved*

electronic record metadata or content.

A.3.18 (M) The RKS must not allow a user to have access to classes, folders or records or their metadata (according to configuration) by means of any search and retrieval function, where the access controls and protective markings allocated to those classes, folders or records prevent access by that user.

A.3.19 (HD) The RKS should be capable of supporting the integration, within the design architecture of RKS[26] of a different search engine from the one with which it is routinely supplied.

Display

A.3.20 (M) The RKS must enable the contents of any or all of the folders or records in a set of search results to be directly displayed without requiring a further search, or re-entry of data already retrieved.

A.3.21 (M) The RKS must routinely be able to display the content of all the types of electronic records which it is able to capture, in a manner that:

- shows all the features of visual presentation and layout as rendered by the generating application package;

- displays all components of an electronic record together as a unit.

A.3.22 (M) The RKS must provide viewing mechanisms capable of displaying all the types of electronic records which it is able to capture, even though the generating application is not present.

A.3.23 (M) The RKS must support simultaneous retrieval and display of classes, folders and records by multiple users.

A.3.24 (M) The RKS must be capable of displaying all available metadata associated with a folder or electronic record on request.

A.3.25 (M) The RKS must be able to print all types of electronic records which it is able to capture, and which are printable, in the same manner as they are displayed on screen within the RKS, without use of 'screen-dumping' or 'snapshots'.

A.3.26 (HD) The RKS should allow all the records in a folder or a part (which are printable) to be printed in one operation.

A.3.27 (HD) The RKS should allow the initial search results – that is, a list of folders or records – to be printed.

A.3.28 (M) The RKS must allow the metadata for a class, folder, and record, to be printed.

---

[26] *i.e. an organisation may wish to implement its standard search engine technology, which is different from that supplied by the RKS*

Presentation

A.3.29 (HD) The RKS should provide facilities for the presentation of folder metadata, records and record metadata to a destination external to the RKS, in a form suitable for electronic publication.

A.3.30 (HD) The RKS should support the selection and presentation of:

- whole classes, including selected elements of class metadata and a list of folders which that class contains;
- whole folders, including selected elements of folder metadata, and a list of record titles which that folder contains;
- specified electronic records, including record content and selected elements of record metadata;
- specified extracts, including record content and selected elements of metadata, but without the record to which the extract is related.

A.3.31 (M) Where the RKS is capable of presentation of classes, folders and records, these must be able to be rendered in one or more of:

- an XML format suitable for publication
- a non-proprietary HTML format suitable for publication
- a GIF approved format suitable for publication.

A.3.32 (HD) The RKS should allow an e-mail retrieved by browsing or searching to be copied to a compatible e-mail application, for transmission in a manner normally achieved by that application.

A.4: RETENTION AND DISPOSAL

Disposal schedules: definition

A.4.1 (M) The RKS must provide a mechanism for the definition and later amendment of a rule base of retention and disposal rules (afterwards called disposal schedules), each of which can be allocated to classes, folders, and record type records.

A.4.2 (M) The RKS must support a unique identifier for each disposal schedule.

A.4.3 (M) The RKS must be capable of restricting the ability to define and maintain disposal schedules in the rule base to authorised users.

A.4.4 (M) The RKS must enable an authorised user to re-define an existing disposal schedule in the disposal schedule rule base, and ensure that the re-definition takes force on all the objects to which that schedule is already allocated.

A.4.5 (M) The RKS must be capable of maintaining a history of changes to disposal rules, the date at which the change was made, and the reason for the change.

A.4.6 (M) The RKS must be able to import and export a set of disposal schedules.

A.4.7 (M) The RKS must support disposal schedules which consist of:

- a retention period, commencement of which is triggered by the effective date of an event type;
- an event type, which determines the commencement of a retention period;
- a set of disposal instructions, which come into force when the retention period is completed.

A.4.8 (M) The RKS must support retention periods which can be expressed as a period of either:

- a number of whole months[27] from one to eleven months
- a number of whole years, from one to 100 years.
- a combination of whole months and years.

A.4.9 (M) The RKS must support the following internal event types which can automatically trigger the commencement of a retention period:

- opening date of a folder
- opening date of a part
- closing date of an folder
- closing date of an part
- last addition (that is, date of creation) of an electronic record to an electronic folder
- last retrieval[28] of an electronic record from an electronic folder
- date of last review of a folder or part.

A.4.10 (M) The RKS must support external event[29] types which can automatically trigger commencement of a retention period which occurs outside the knowledge of the system, and must:

- enable an authorised user to notify the RKS that a specified event has occurred;

---

[27] *Months may be expressed as a total number of days*

[28] *'Retrieval' means that the record content has been viewed by an end user by the facilities provided by the RKS for this purpose in normal operation*

[29] *i.e. an event which occurs outside the knowledge of the system, and which is notified to the system by an operator*

- enable an authorised user to notify the RKS of the effective date on which the event occurred;

- automatically trigger the retention period when notification of the event is received by the RKS, without requiring explicit amendment of each disposal schedule which is activated.

A.4.11 (M) The RKS must be able to accept definition of more than one external event, each of which may be used separately by different schedules allocated to different groups of folders.

A.4.12 (M) The RKS must support the allocation of disposal instructions as part of a disposal schedule which include:

- review
- export
- transfer (i.e. export, followed by destruction)
- destruction.

A.4.13 (HD) The RKS should support staged disposal by enabling the definition of multiple stages within a single disposal schedule; for each stage it must be possible to define a sequence of separate pairs of disposal dates and actions, each of which will come into force in turn.

Disposal schedules: allocation

A.4.14 (M) The RKS must provide a mechanism for the allocation of a pre-defined disposal schedule to each class, electronic folder and specified record_types in the RKS, by selecting from the current defined set of schedules in the rule base.

A.4.15 (M) The RKS must enable, but not require, the allocation of a disposal schedule to a class, to be, by default, inherited downwards by all folders subsequently created under that class (i.e. inheritance on creation).

A.4.16 (M) The RKS must enable a disposal schedule to be allocated to any specific folder, that is different from and can take precedence over (i.e. over-rides), a disposal schedule which may have been inherited from a class. Application of this function must be consistent with the requirements for resolution of disposal conflicts set out below.

A.4.17 (M) The RKS must be capable of restricting the ability to allocate and re-allocate disposal schedules to folders and classes, to authorised users.

A.4.18 (HD) The RKS should support the ability to allocate a disposal schedule to a pre-defined record type which has been defined at configuration as capable of supporting this action (i.e. which is not the default record type); and if so, must ensure that the capability to allocate such as schedule can be restricted to authorised users.

A.4.19 (HD) The RKS should ensure that where a specific disposal schedule has been allocated to a record type, each instance of a record created under that type will inherit the schedule at

the time of record creation, regardless of the folder to which it is allocated. (Example: Performance Appraisal record)

Hypothetical example:
*A **Disciplinary Warning** allocated to the personnel folder for an individual should normally be removed from the folder after a period of 6 months.*
*A **Disciplinary Warning record type** should allow records created under that type to have an appropriate schedule inherited automatically, which will be different from the schedule allocated to the folder as a whole.*

A.4.20 (M) Where the RKS does not support automatic inheritance of a disposal from a record type to all instances of records created within that type, the RKS must:

- enable a disposal schedule to be allocated to an individual instance of a record type which allows this capability, *but not* to the standard default record type (which does not);

- *and* must ensure that the capability to allocate such as schedule can be restricted according to user role.

A.4.21 (M) The RKS must enable an authorised user to re-allocate a different disposal schedule to an existing folder or class, where that folder or class already has a disposal schedule allocated, at any point in the life of the folder or class.

A.4.22 (HD) Where a disposal schedule is re-allocated to an existing class, from which one or more folders or classes have inherited a disposal schedule, the RKS should ensure that the new schedule is inherited by those folders or classes which previously inherited a schedule from that class, except for any where a different and over-riding schedule has been individually allocated (i.e. retrospective inheritance).

A.4.23 (HD) Where a disposal schedule is re-allocated to an existing electronic Record type, under which records of that type have inherited a disposal schedule, the RKS should ensure that the new schedule is inherited by those records which previously inherited a schedule from the record type.

A.4.24 (M) When a schedule is re-allocated, or a folder or group of folders is moved from one class to another, the RKS must *either*:

- offer an option to automatically replace the existing schedules inherited from the source class with schedules to be inherited from the destination class, and to notify of exceptions for manual decision, *or*

- provide an immediate entry into a disposal re-scheduling process in order to manually change all necessary schedules as required.

A.4.25 (M) The RKS must enable a disposal hold to be placed on a folder or group of folders by an authorised user, which has the effect of pausing the disposal process (i.e. no disposal action can be taken on the folders and the records contained while the hold is in place).

A.4.26 (M) The RKS must prevent any folder or record which has a disposal hold placed on it from being deleted by an Administrator, outside of the disposal process.

A.4.27 (M) The RKS must be capable of reporting on folders and records which have a disposal hold placed on them, and enable such a hold to be removed by an authorised user only.

A.4.28 (HD) The RKS should maintain a history of disposal schedule rules that have been applied to each folder, class or record type as metadata with the folder, class or record type.

Disposal execution

A.4.29 (M) The RKS must automatically track the commencement and progress of retention periods, on all folders and records which have been allocated disposal schedules, in order to determine effective disposition dates.

A.4.30 (M) The RKS must provide a disposal management mechanism, which will, once the disposal process is initiated by an authorised user:

- automatically identify all qualifying folders and records where the specified conditions for disposal are fulfilled;
- notify an authorised user of all the folders and records so qualifying;
- enable re-allocation of a disposal schedule to folders if required, which then determines whether the folders currently qualify for disposal, and
- carry out the disposal action on confirmation to proceed.

A.4.31 (M) The RKS must ensure that the all actions required by a disposal schedule are applied to all the contents of the folder as a whole, unless a separate disposal schedule for one of its constituent records has been allocated[30] by use of a specific record type which allows this action.

A.4.32 (M) The RKS must always seek confirmation before implementing disposal actions.

A.4.33 (D) The RKS should seek confirmation of irreversible actions twice before proceeding.

A.4.34 (M) The RKS must ensure that all functions of the disposal management mechanism are restricted to authorised users.

---

[30] *It is not intended that a destruction or export action should take place at the folder level at an earlier date than an action scheduled for a contained record (i.e. the folder should have a longer life than a differently scheduled record which it contains). The RKS disposal allocation mechanism should helpfully include checks to prevent such situations occurring*

A.4.35 (M) The RKS must ensure that, in normal operational conditions, a disposal schedule allocated to any folder is triggered by the system date, and can only become effective in real time[31] (i.e. that the disposal schedule cannot be triggered by artificially advancing the current date within the disposal management mechanism).

A.4.36 (M) Where the contents of a metadata field are used by a disposal schedule to determine a disposal date, the RKS must be capable of tracking any changes made to the contents of that field and re-determining the disposal date once a change is made, after initial allocation of the schedule.

A.4.37 (M) When processing a folder which is allocated a disposal schedule that uses the opening or closing date of a part as the event type which triggers the schedule, the RKS must apply the disposal action to the specific part which was opened or closed (and thereby triggered the event), and must not apply the disposal action to any other parts in the folder, or to the whole folder.

A.4.38 (M) The RKS must be capable of identifying folders and records which have a disposal hold placed on them, so that any disposal action is not carried out while the hold is in force.

Resolving conflicts

A.4.39 (M) The RKS must at all times ensure that, where a folder is governed by more than one disposal schedule, at the individual folder and at the class levels, which may specify conflicting disposal actions, execution of a disposal action is moderated by the requirements of all other schedules that pertain, so that:

- the most specific schedule (the lowest in the hierarchy) applies;
- resolving a disposal conflict must not ever result in a folder which does not yet qualify for disposal becoming 'disconnected' from the class hierarchy by the removal of intermediate structure;
- a Review action takes precedence over a Destroy or Export action, and
- an Export action takes precedence over a Destroy action.

A.4.40 (M) Where an electronic record is governed by more than one disposal schedule because the record is assigned to more than one electronic folder, (for example, using a pointer scheme), the RKS must automatically track all retention periods and disposal actions that are applicable and ensure that the record is unfailingly retained within each folder where it is required, for the retention period which applies to that folder, so that:

- removal of the record from visibility in one folder at an earlier date does not prejudice continued inclusion of that record in another folder until a later date;

[31] *i.e. the time as defined by the system server (not the client).*

- continued inclusion of a record in one folder until a later date does not preclude the removal of that record from another folder where the retention period is shorter; and that in such a case, the record is removed from the folder with a shorter retention period.

A.4.41 (M) The RKS must at all times ensure that, where a record is governed by more than one disposal schedule, one at the folder level and the other at the record_type level, which may specify conflicting disposal actions:

- the record type schedule, allocated to the individual electronic record because it falls within a specific record type, takes precedence over the schedule allocated to the folder to which that record is assigned, where this calls for destruction or review of the record earlier than destruction or review of the folder;

- destruction of the individual record has no secondary effect on the remaining contents of the folder, other than removal of that record;

- destruction of the folder before destruction of the individual record is due, is not possible, and that an authorised user is notified of this conflict either at time of schedule allocation or at time of attempted disposal.

A.4.42 (M) The RKS must at all times ensure that, where a single record is allocated to more than one folder by means of a pointer system, and that record is governed by several disposal schedules, at both the individual folder level and at the record type level, which may specify conflicting disposal actions:

- the record type schedule, allocated to the individual electronic record because it falls within a specific record type, takes precedence over all schedules allocated to any folders to which the record is assigned, where this calls for destruction or review of the record earlier than destruction or review of the folder;

- destruction of the individual record removes the record from all folders to which it is allocated, but has no secondary effect on the remaining contents of the folder, other than removal of that record;

- destruction of a folder to which the record is allocated, before destruction of the individual record is due, is possible as long as the record remains allocated to another folder, but that this action requires notification to and explicit confirmation by an authorised user, or

- destruction of the last remaining folder to which a record is allocated before destruction of the individual record is due, is not possible, and that an authorized user is notified of this conflict either at time of schedule allocation or at time of attempted disposal.

A.4.43 (M) The RKS must ensure that all conflicts in disposal actions are resolved by either:

- automatically applying the strictest schedule according to precedence in the above requirements and alerting an authorised user of this fact if necessary;

- notifying an authorised user of the conflict and presenting the available options for immediate resolution.

Review

A.4.44 (M) When a disposal schedule triggers a review disposal action on an electronic folder or class, the RKS must enable the re-allocation of a disposal schedule, which may result in:

- a later review, following a further retention period;
- marking for permanent preservation and transfer to the United Nations Archives, immediately or following a further retention period;
- destruction, immediately or following a further retention period.

A.4.45 (M) The RKS must make all metadata for a folder or class scheduled for review available to the reviewer.

A.4.46 (M) The RKS must make all the contents of a folder or class scheduled for review available to the reviewer on request, within access control restrictions.

A.4.47 (M) The RKS must ensure that immediate destruction within the disposal process can only be achieved by re-allocation of a schedule that explicitly authorizes this action[32].

A.4.48 (M) The RKS must support the progressive addition of metadata through iterative review processes, and must enable the reason for the outcome of that review to be recorded as folder metadata.

A.4.49 (HD) The RKS should automatically record the date of last review of a folder, so that it can be used as the trigger of a disposal rule.

Export and transfer

A.4.50 (M) The RKS must be able to export electronic folders, folder and class metadata, all their constituent electronic records and the record metadata, for import to another RKS, or for transfer to ARMS for permanent preservation.

A.4.51 (M) Whenever the RKS exports any class, folder, or part, the RKS must be able to export:

- all folders which qualify under the disposal action
- all parts in the folder(s) which are to be exported

---

[32] *That is, there is no separate delete function in the review process; allocation of a schedule for immediate destruction must cause the folder to enter the standard disposal management process for destruction*

- all records in all folders and parts which are to be exported
- all metadata associated with folders, parts and records which are to be exported.

A.4.52 (M) The RKS must be able to export whole electronic folders, and groups of folders, and all associated 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 clearly linked to the record to which it belongs, so that the correct metadata can be re-associated with the correct record in the receiving system;

- all structural links between records, parts, folders and classes are retained in such a way that the structure of all linked components qualifying for export can be re-built in a receiving system.

A.4.53 (M) The RKS must be able to export and transfer records that are associated with more than one folder, where this is achieved by means of a pointer, ensuring that:

- in a folder to be exported, a physical rather than virtual instance of the record is exported, resulting in an exported record not an exported pointer;

- in a folder that is not to be exported, the evident association of the record with that folder, and access to the content of the record, remains unaltered;

- where associated with two or more folders qualifying for export, all associations between the record and all exported folders are retained in the exported data.

A.4.54 (HD) The RKS should be able to include a copy of audit trail data that is associated with records, parts and folders as part of the export or transfer process; and must then exclude n on-relevant audit trail data.

A.4.55 (M) The RKS must be able to export metadata for folders, parts and records in a (to be determined) standard format.

A.4.56 (M) The RKS must be able to support the export of metadata in a standard format as defined by the record-keeping metadata standard schema, as versions become available through ARMS, and in accordance with the schedule for compliance.

A.4.57 (M) The RKS must also be able to export records:

- in their native format, or a current format to which they been migrated and in order of preference:

- in a standard format where possible;

Such renditions may be achieved by:

- capturing an appropriate rendition as part of the record capture process
- rendering the record as part of the export process
- exporting directly to another package which is capable of rendering the record within a controlled environment.

A.4.58 (M) The RKS must be able to export all types of records which it is able to capture, regardless of the presence of the generating application software.

A.4.59 (HD) The RKS should be able to export all folders, and groups of folders, that qualify for export at any one time, in one single sequence of steps[33].

A.4.60 (M) The RKS must produce a report detailing any failure completely to export or transfer any element of electronic records, parts and folders and associated metadata that are being processed in the disposal management mechanism which must identify any records which have generated processing errors during export or transfer, and any folders, parts or records that have not successfully been exported.

A.4.61 (M) The RKS must enable folders, parts and records to be exported more than once.

A.4.62 (M) The RKS must support a two-stage transfer process, consisting of:

- export of qualifying folders, part and records from the system;

- subsequent destruction of the exported folders, parts and records following confirmation of export.

A.4.63 (M) The RKS must retain intact all electronic folders, parts and records that have been exported in the transfer process, at least until confirmation of a successful export (i.e. pause the second stage of the process until confirmation of successful import to the recipient system following the first stage).

Destruction

A.4.64 (M) The RKS must seek confirmation of destruction from an authorized user as a mandatory step in the disposal process, before any action is taken on folders, parts or records; and enable cancellation of the disposal process at this point if confirmation is not given.

A.4.65 (M) The RKS must ensure that any function to delete records, parts or folders on an ad hoc basis (outside of the disposal process) is restricted to only the highest level of Administrator.

A.4.66 (M) The RKS must distinguish between an ad hoc delete function, and the destruction function within the disposal process, so that each can be individually and discretely allocated to differing sets of authorized users as separate functions.

---

[33] *That is, in one pass through the disposal process, although some minor iteration is acceptable*

A.4.67 (M) Where records are stored on re-writeable media, the RKS must enable the complete obliteration[34] of records, parts, folders, and groups of folders that have been so scheduled and confirmed, so that they cannot be restored by operating system features[35] or by specialist data recovery facilities.

A.4.68 (M) Where records are stored on write-once media, the RKS must prevent access to them so that access cannot be restored by normal use of the RKS, by standard operating system utilities, or by any other application.

A.4.69 (HD) The RKS should be capable of retaining a minimum set of metadata associated with destroyed folders, as specified in the accompanying records management metadata standard.

A.4.70 (HD) Where destruction is initiated from a higher level in the hierarchy, the RKS should ensure that the correct minimum metadata is retained for all destroyed folders[36].

A.4.71 (HD) Where a folder is deleted by an Administrator, the RKS should ensure that the correct minimum metadata is retained; and that the Administrator has an opportunity to enter the reason for destruction in an appropriate metadata field.

A.4.72 (HD) The RKS should provide a facility for an Administrator to optionally archive[37] and then delete minimum metadata for destroyed folders.

A.4.73 (M) Where a pointer system is used, the RKS must maintain complete referential integrity following all destruction processes, consistent with all the requirements in this section.

A.4.74 (M) The RKS must ensure that when a destruction process is applied to any record for which the RKS also stores alternative renditions, all renditions of the record are also destroyed.

5. ACCESS CONTROL

Access to RKS

A.5.1 (M) The RKS must provide an authentication mechanism which controls access to the RKS and which validates each user attempting access at the start of each user session, linking the user-id to a valid user profile. An individual user-id/password login is the minimum strength requirement for authentication.

---

[34] *For example, to the specification of the US Department of Defense standard <ref.*

[35] *Excluding disaster recovery facilities, controlled by procedure*

[36] *for example, where a set of folders under a higher level class are destroyed, minimum metadata is individually retained for all folders in all classes descendant from that*

[37] *i.e. take a copy which is outside the RKS control*

A.5.2 (HD) The RKS should enable configuration of an access mechanism which supports access to the RKS system by an integrated network log-in.

A.5.3 (M) The RKS must allow:

- new users to be defined and identified
- existing users to be marked as inactive, with the effect of barring that user from subsequent entry to the RKS
- existing users to be deleted by an Administrator at any time.

A.5.4 (HD) The RKS should allow a user to be defined with administration rights over only a section of the classification scheme; that is, define a local records officer.

Access control markings

A.5.5 (M) The RKS must support the definition of all access control markings required prior to their allocation to a user, class, folder or record.

A.5.6 (M) The RKS must restrict the ability to define and maintain available access control markings to an Administrator.

A.5.7 (M) The RKS must grant to each user the ability to allocate to folders and records the access control markings (which have already been defined) which that user has been allocated as access permissions.

A.5.8 (M) The RKS must not allow the allocation to folders and records of access controls by any users who are not themselves allocated those same access permissions.

A.5.9 (M) The RKS must support use of a protective marking scheme in order to control which users are allowed access to which records, folders and classes, consisting of a hierarchy of security categories of at least five levels, from unrestricted access at the lowest level to highly restricted access at the highest level.

A.5.10 (M) The RKS must support use of access control markings which identify:
pre-defined groups of users, and separately individual users in order to control which users are allowed access to which electronic records, folders and classes.

User profiles

A.5.11 (M) The RKS must require the definition of a user profile for each user known to the system. A user profile must always identify a functional role for the user, and must enable allocation of access control markings to that user; and must require information necessary for valid authentication (for example, user-id and password).

A.5.12 (M) The RKS must support the allocation of a single security category and membership of multiple pre-defined access groups, recorded in the user profile for each user known to the system; and must restrict the ability to allocate these markings to an Administrator.

A.5.13 (M) The RKS must require each user to be allocated exactly one hierarchical security category, with the default category being the lowest level of the hierarchy.

A.5.14 (M) Where an RKS enables a security category to be inherited from a role, the RKS must ensure that a different security category can be allocated at the individual user level to replace it.

A.5.15 (M) The RKS must enable each user to be allocated membership of multiple predefined groups; but must not require a user to be a member of any pre-defined groups[38].

A.5.16 (M) The RKS must allow changes to be made to a user profile at any time, and must restrict this ability to an Administrator.

Roles

A.5.17 (M) The RKS must support the definition of a set of user roles, which control the assignment of rights to specific functions or groups of functions; and must restrict any ability to define or customize these roles to an Administrator.

A.5.18 (M) The RKS must ensure that all users are allocated to one or more user role(s). A.5.19 (M) The RKS must be able to limit access to system functions and facilities, so that all users will only be able to carry out those functions which are permitted by the user role(s) to which they have been allocated.

A.5.20 (M) The RKS must support a model of user roles that enables functions to be allocated to user types.

A.5.21 (HD) The RKS should enable the allocation of a security category, and predefined access control group membership, to a role so that all users allocated to that role automatically inherit the access permissions of the role, and if so must ensure consistent rules of precedence between permissions granted at the role and at the individual user level.

Groups

A.5.22 (M) The RKS must support the definition of pre-defined access control groups which identify business or other functional groups, so that, in principle, any user can be a member of any group, and differing groups at differing times; and must restrict this ability to allocate and reallocate to an Administrator.

A.5.23 (M) The RKS must allow:

- new groups to be defined
- existing groups to be marked as inactive, which should have the effect of barring access previously allowed by that group marking.
- existing groups to be deleted.

---

[38] *Excluding a global 'Everyone' group*

A.5.24 (M) The RKS must enable any user to be added to or removed from groups at all times.

A.5.25 (HD) The RKS should enable, but not require, the allocation of a class to a group, so that all users allocated to that group are only granted access to that class and its sub-classes (i.e. to that section of the record plan).

Allocation of access control to classes, folders and records

A.5.26 (M) The RKS must support the allocation of all forms of access control markings to classes, folders and electronic records, including:

- security categories (protective markings)
- pre-defined access control groups, (that is, a stable list of named users)
- one or more individual usernames (that is, an *ad hoc* list of named users)

A.5.27 (M) The RKS must enable any and all combinations of protective marking, predefined user groups and individual usernames to be allocated to classes, folders and records.

A.5.28 (M) The RKS must ensure that an electronic part will always inherit the access control markings allocated to the folder which it segments.

A.5.29 (M) The RKS must enable exactly one security category to be allocated to a class, electronic record or folder, with the default category automatically being the lowest level of the hierarchy.

A.5.30 (M) The RKS must ensure that all folders created under a class inherit a security category allocated to that class by default, unless explicitly overridden at the folder level.

A.5.31 (M) Where a folder has a higher security category, the RKS must be capable of automatically upgrading the security category of a record with a lower rating to that of the folder in which it is contained.

A.5.32 (HD) The RKS should allow a configuration option, to be set by an Administrator, which allows a record to have a lower level security category than the folder in which it is contained.

A.5.33 (M) The RKS must be capable of automatically upgrading the security category of a folder to the level of the highest rating of any its contents.

A.5.34 (HD) The RKS should allow a configuration option, to be set by an Administrator, which allows a record to have a higher level security category than the folder in which it is contained[39]

A.5.35 (M) The RKS must allow the addition of a descriptor to an electronic folder or record as an element of metadata, for informative use[40]

[39] *All requirements relating to the control of access by users must apply consistently within these configuration options*

A.5.36 (M) The RKS must support the amendment of access control markings on classes, folders and records.

A.5.37 (HD) The RKS should retain the previous access control marking(s), and the date of the amendment, as an historical metadata element for that class, folder or record.

A.5.38 (HD) The RKS should support the allocation of a security category to a class, folder or record, which is valid for a limited time period, and should automatically downgrade the marking to the lowest level security category when the time period has expired.

A.5.39 (D) The RKS may support the allocation of a security category to a class, folder or record, which is valid for a limited time period and should automatically downgrade the marking to a lower, pre-selected, security category when the time period has expired.

A.5.40 (D) The RKS may support notification to an authorised user of the expiry of a selected time period for which a security category has been allocated to a class, folder or record, and allow the security marking to be reassessed and amended.

Custodian

A.5.41 (M) The RKS must enable, but not require, a user or group to be identified as the responsible custodian for an electronic folder, and enable this identification to be changed at a later date.

A.5.42 (M) The RKS must be able to limit access to an electronic folder or record solely to an identified responsible custodian of that folder or record.

A.5.43 (M) The RKS must allow a responsible custodian to limit access by stipulating which other users or groups can access records of which the user is custodian.

A.5.44 (M) The RKS must be capable of restricting the ability to allocate and amend access control markings (including the ability to add or remove users and groups) on electronic folders and records to the responsible custodian of the folder where one is identified, with the exception of an Administrator.

Execution of access control markings

A.5.45 (M) The RKS must allow all users (unless otherwise restricted by functional role) access to all classes, folders and records which are not allocated an access control marking other than the lowest security category[41]

---

[40] *Access control functionality is implemented by user group and individual lists, descriptors give a reason for this control*

[41] *That is, those allocated an Unclassified security category*

A.5.46 (M) The RKS must limit access to classes, folders and records which have been allocated a security category, only to those users who have been allocated an equivalent or higher security category.

A.5.47 (M) The RKS must limit access to classes, folders and records which have been allocated a pre-defined access control group, only to those users who are members of that group.

A.5.48 (M) The RKS must limit access to classes, folders and records which have been allocated more than one pre-defined access control group, only to those users who are members of the allocated groups[42].

A.5.49 (M) The RKS must limit access to classes, folders and records which have been allocated one or more individual usernames as access control markings, only to those users so named.

A.5.50 (M) The RKS must limit access to classes, folder and records which have been allocated one or more forms of access control marking, only to users who have also been allocated all[43] equivalent access control markings; and prevent access by users who have been allocated some, but not all, the equivalent access control markings[44].

A.5.51 (HD) The RKS should include a configuration option which defines the behaviour of the access control mechanism so that:

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

A.5.52 (M) The RKS 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 on record content, which that user would not receive through searching on metadata.

---

[42] *i.e. a clear and consistent approach should be taken to implement this requirement, for example configuration option offered whether ownership of all or any of the groups is necessary for access*

[43] *For example, a user with a security category of Confidential normally has access to records marked Confidential or Restricted (lower in the hierarchy); but not to records marked Restricted and also allocated a Budget access control group (caveat)*

[44] *In the case of a pre-defined access control group, and one or more individual usernames, co-existing as access control markings, a user may be granted access if either a member of the group, or listed as an individual username. Here, a list of individual usernames extends, rather than restricts, membership of the pre-defined group.*

A. 6. AUDIT

A.6.1 (M) The RKS must be able to automatically record an audit trail of events under the control of the RKS, storing information about:

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

A.6.2 (M) The RKS must be able to record in the audit trail all changes made to:

- groups of electronic folders
- individual electronic folders
- electronic parts
- electronic records
- extracts metadata associated with any of the above.

A.6.3 (M) In particular, the RKS must be capable of recording information in the audit trail about the following events:

- the date and time of creation of all electronic records;
- re-location of an electronic record to another electronic folder, identifying both source and destination folders;
- re-location of an electronic folder to a different class, identifying both source and destination classes;
- re-allocation of a disposal schedule to an object, identifying both previous and reallocated schedules;
- placing of a disposal hold on a folder;
- the date and time of a change made to any metadata associated with electronic folders or electronic records;
- changes made to the allocation of access control markings to an electronic folder, electronic record or user;
- export actions carried out on an electronic folder;
- separately, deletion or destruction actions carried out on an electronic folder or electronic record, by all users including an Administrator.

A.6.4 (M) The RKS must track and record information about events in the audit trail without manual intervention, once the audit trail facility has been activated.

A.6.5 (M) The RKS must ensure that audit trail data cannot be modified in any way, or any part of the data be deleted by any user, including an Administrator.

A.6.6 (HD) The RKS should allow the extent of audit trail tracking and recording to be user-configurable, so that an Administrator can select the events for which information is automatically recorded; the RKS must ensure that a minimum level of events includes: Create, Edit (If allowed), Copy, Move, Delete, Destroy, Export.

A.6.7 (M) The RKS must ensure that the selection for audit trail tracking, and all later changes to it, are also recorded in the audit trail.

A.6.8 (M) The RKS 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.

A.6.9 (M) The RKS 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[45] who have little or no familiarity with the system.

A.6.10 (M) The RKS must maintain a log of failed attempts to log-on to the RKS.

A.6.11 (M) The RKS must be capable of producing ad hoc reports selecting all relevant information from the audit trail for:

- actions carried out by a specified user, or group of users, during a specified date and time period;
- actions carried out on a specified folder, or group of folders, during a specified date and time period;
- actions carried out on a specified record, during a specified date and time period.

A.6.12 (HD) The RKS should be able to export an audit trail, or parts of an audit trail, for specified electronic records, electronic folders and groups of folders, in such a way that the exported data can itself be stored as a record.

A. 7. REPORTING

A.7.1 (M) The RKS must provide a reporting capability, for Administrators and other authorized users[46] to provide management and statistical reports on activity and status within the RKS.

A.7.2 (HD) The RKS should be capable of storing standard reports requests and formats, which can be run specifying varying parameters, but without additional design alteration, including parameters for:

- specific dates and date ranges

[45] *For example, external auditor*

[46] *The RKS may also provide some general reporting capabilities to end users*

- specific users or groups of users.

A.7.3 (M) The RKS must be able to produce reports listing all classes, folders and parts, structured according to the hierarchy of the record plan.

A.7.4 (M) The RKS must be able to produce reports listing all classes, folders and parts within a section of the record plan only.

A.7.5 (M) The RKS must be able to produce reports listing all, or a restricted set of, user profiles known to the system.

A.7.6 (M) The RKS must allow reports to be generated for screen display, for printing, and for both display and printing.

A.7.7 (M) The RKS must support reporting tools for the provision of statistics on the activities of users within the RKS, 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 created by a user or groups of users, within a given period.
- the number of electronic records viewed by a user or group of users, within a given period.

A.7.8 (M) The RKS must support reporting tools for the provision of statistics on aspects of electronic records in the RKS, including:

- the number and location of electronic records by application type and application package version;

- the size and capacity of electronic record stores and repositories;

- the number and location of electronic folders and records by specific access control markings.

A.7.9 (M) The RKS must support reporting and analysis tools for the management of retention and disposal schedules, including:

- folders and records with disposal schedules which will come into force over a given period of time, providing quantitative reports on the volume and type of records;

- statistics of review decisions made over a given period;

- a list of all disposal schedules that are currently defined in the disposal schedule rule base;

- a list of all classes and electronic folders to which a specified disposal schedule is currently allocated;

- all disposal schedules which are currently allocated to a class, groups of classes, or group of folders;

- all disposal schedules which are currently allocated to a record created as a specific record_type;

- a list of all folders for which a specified disposal action will be required over a given period whether this information is inherited or individually allocated.

A.7.10 (M) The RKS must be capable of producing reports documenting the outcome of the export process which list classes and folders successfully exported as a record of a specific export action.

A.7.11 (M) The RKS must be capable of producing reports documenting the outcome of the destruction process, which list classes and folders successfully destroyed.

A. 8: USABILITY

A.8.1 (M) The RKS must follow the accepted standard rules for the user interface of each operating system or platform for which it is supplied[47].

A.8.2 (M) The RKS must consistently present user interface menus, commands and other facilities in all parts of the application.

A.8.3 (M) The RKS must use consistent terminology to label functions and actions in all parts of the application.

A.8.4 (M) Where a web browser interface is employed, the RKS must be consistent with the United Nations' guidelines for web design.

A.8.5 (HD) The RKS should provide a context-sensitive online help facility.

A.8.6 (D) The RKS may allow customization of the contents of the help facility, by the addition of new, or editing of existing, text.

A.8.7 (M) The RKS must produce error messages which are meaningful and appropriate, and should offer immediate prompts for actions to resolve the error wherever possible.

A.8.8 (M) Where validation errors are detected, the RKS must unambiguously describe the nature of the error, and offer a method of correcting the error, or cancelling the action.

A.8.9 (HD) The RKS should be capable of removing the visibility of functions from users who do not have access to those functions in their allocated user role.

---

[47] *For example, a Windows-based version of an RKS should follow Microsoft Official Guidelines for User Interface Developers and Designers, and a Macintosh-based version of the same RKS should follow Apple User Interface Guidelines*

A.8.10 (HD) The RKS should not, routinely, allow the intermediate steps of a function to be carried out if the user will not be allowed to complete the function because that function is disallowed by role allocated to that user.

A.8.11 (M) The RKS must provide facilities for end users and Administrators which are intuitive and easy to use, and require as few actions as possible to carry out the function to the required standard; in particular, in normal operation, the RKS must be able to:

- capture and create (apart from selection of a folder or entry of metadata attributes) a record within three mouse clicks or keystrokes;
- be capable of presenting all mandatory metadata elements for record capture with minimum demands on the user;
- display the contents of a record from a search result list within three mouse clicks or keystrokes;
- display metadata for a folder or record within three mouse clicks or keystrokes.

A.8.12 (M) Where on-screen windows are employed, the RKS must ensure that where an end user is able to re-size and re-locate windows, the contents of those windows remain correctly aligned.

A.8.13 (M) The RKS must support multiple simultaneous display[48] of folders and records.

A.8.14 (HD) The RKS should support a 'drag and drop' method of manipulating folders and records, where this is appropriate for the platform supported[49].

A.8.15 (HD) The RKS may support the ability to define multiple user views of the class and folder structure, with no effect on the common corporate record plan structure.

A.8.16 (HD) The RKS should be usable with a wide range of common accessibility software features[50].

A.8.17 (D) The RKS may support the use of, and navigation by, hyperlinks and other cross-references that are contained in records at time of creation.

A.8.18 (HD) The RKS should automatically present default values for data entry fields where logically possible, and as specified in the accompanying records management metadata standard.

---

48 *For example, by use of tiled or overlapping windows*

49 *For example, in capturing a record into the RK*

50 *See" Keeping Technology Dependent Records Accessible" Document for common examples*

A.8.19 (HD) The RKS should support the pre-definition of a set of allowed values for a particular metadata field by an Administrator, and the implementation of these values as a selection list (i.e. a 'pick list').

A.8.20 (M) The RKS must provide an interface to standard e-mail clients, which enables e-mail messages to be captured directly into the RKS from the e-mail client.

A.8.21 (M) The RKS must be capable of integrating with the standard office system packages which the RKS supports, so that the record can be captured by the RKS by use of the Save facility.

A.8.22 (M) The RKS must be capable of generating an e-mail message from within the application in order to attach, as options:

- one or more records stored in the RKS (in the same message)
- active pointer(s)[51] to one or more records stored in the RKS
- metadata for one or more records stored in the RKS.

A. 9: DESIGN AND PERFORMANCE

A.9.1 (M, A) The RKS must provide a robust and flexible architecture that can evolve to meet the needs of a changing organizational environment, appropriate to the types of implementation for which the RKS is intended

Integrity

A.9.2 (M) The RKS must enforce data integrity, referential integrity and relational integrity at all times.

A.9.3 (M) The RKS must ensure that all occurrences of classes, folders, records, parts and extracts are allocated a system identifier which is unique within the system.

A.9.4 (HD) When the RKS automatically generates an identifier which is available for meaningful operational use by a user or Administrator, the RKS should allow an Administrator to configure the pattern and starting number(s) or character(s).

A.9.5 (M) The RKS must store calendar years in a four digit format (YYYY) in any metadata field that contains a date.

A.9.6 (M) The RKS must be capable of storing dates that refer to years in the previous, current and subsequent centuries, and must correctly process these dates at all times.

[51] *In the sense of 'shortcuts'.*

Interfaces

A.9.7 (M, A) The RKS must support a remote log-in facility, which provides the standard range of functionality which the RKS offers.

A.9.8 (HD, A) The RKS should provide an interface to:

- one or more low volume, ad hoc, scanning system(s);
- one or more high volume production scanning system(s).

A.9.9 (D, A) The RKS may provide an interface to one or more image management system(s).

A.9.10 (D, A) The RKS may provide an interface to a fax server facility.

Disaster recovery

A.9.11 (M, A) The RKS must support automated back-up and recovery facilities for all classes, folders, records, metadata, audit trails and configuration settings held in the RKS, either provided by the RKS itself or by facilities in its environment with which it can interface.

A.9.12 (M, A) The RKS must support a capability for separate physical storage of back-up data[52]

A.9.13 (HD, A) The RKS should allow an Administrator to:

- specify the frequency of back-up;
- select elements of the RKS to be backed-up.

A.9.14 (M, A) The RKS must support facilities for an Administrator to restore the whole RKS from back-ups following a system failure.

A.9.15 (M, A) The RKS must support facilities for an Administrator to restore the whole RKS from the most recent back-up state to the point of system failure[53].

A.9.16 (M, A) The RKS must be able to determine any updates to the data which are unable to be restored / rebuilt, and provide notification to an Administrator.

A.9.17 (M, A) The RKS must support restoration of audit trail information by means of the back-up and recovery facilities.

---

[52] *i.e. it must be possible to store back-up date separately from the RKS itself*

[53] *For example by forward build, RAID / server clustering or other appropriate technology*

Storage

A.9.18 (HD, A) The RKS should support a distributed repository with multi-site service.

A.9.19 (HD, A) The RKS should support caching of frequently and recently used repository content.

A.9.20 (HD, A) When querying a remote repository, the RKS should minimise the amount of data exchange required.

A.9.21 (M) The RKS must provide facilities for monitoring storage facilities, and automatically alert an Administrator when a capacity threshold is reached, or when an error condition requiring attention occurs.

Performance

A.9.22 (M, A) The RKS must provide evidence of adequate performance and response times for commonly performed functions under the normal operating conditions for which it is intended. A benchmark for normal operating conditions is:

- 75% of the user population actively using the system
- total record volume to be expected after 5 years use stored
- multiple, concurrent and representative active use of system functionality.

Benchmark metrics for performance are:

- time taken to display a graphical view of the class and folder structure
- time to store a set of standard documents at capture and/or creation
- time to return a search response for a simple search
- time to return a search response for a complex (Boolean) search
- time to display a recently captured record
- time to display an 'inactive' record.

Scalability

A.9.23 (M, A) The RKS must provide evidence of the degree of scalability that it can support over time, as organisational needs change and develop. Benchmark metrics for scalability are:

- number of geographical locations at which users can be supported, while maintaining the performance metrics demonstrated;

- total size of the record repository which can be supported, in Gigabytes or Terabytes, while maintaining the performance metrics demonstrated;

- number of total users which can be supported, while maintaining the performance metrics demonstrated;

- systems management overhead in maintaining a growth rate for the number of records and users anticipated in the first five years of operation;

- amount of re-configuration and downtime required to maintain a growth rate for the number of records and users anticipated in the first five years of operation;

- amount of re-configuration and downtime required to make bulk changes to organisational structures, class and folder structures, and user roles with the number of folders, records and user anticipated after five years of operation.

A. 10: COMPLIANCE WITH OTHER STANDARDS

A.10.1 (M, A) Wherever relevant, the RKS must comply with, or support compliance with, the following standards:

- ARMS Standard for Record-keeping Metadata
- ARMS Manual for the Design and Implementation of Record-keeping Systems
- ISO 17799 / BS7799 Information Security Management
- ISO 15489 Information and Documentation : Records Management
- ISO 9001 : 2000 Quality management systems : Requirements.

These contextual standards form the framework within which these RKS requirements operate.

A.10.2 (HD, A) Wherever relevant, the RKS should comply with, or support compliance with, the following standards:

- ISO 23950 Information and Documentation : Information retrieval (Z39.50) : application service definition and protocol specification;

- ISO 2788 Documentation : Guidelines for the establishment and development of monolingual thesauri;

- ISO 5964 Documentation : Guidelines for the establishment and development of multilingual thesauri;

- ISO 9075 Information technology: database languages: SQL.

These contextual standards form the framework within which these RKS requirements operate.

B: OPTIONAL MODULES

Optional modules are not a mandatory part of the core Electronic Records Management requirements. An RKS may fulfil the core requirements without fulfilling any optional module requirements. However, if an RKS wishes to demonstrate a capability of providing one or more of the areas covered by optional modules, within the context of electronic record-keeping, it must fulfil all of the mandatory requirements in that module.

For example, an RKS which fulfils mandatory requirements in Document Management and Hybrid and Physical File Management (as well as the Core Requirements in section A) will have demonstrated compliance as an RKS with integrated document and physical file management capability.

All compliant RKS must always fulfil the Core Requirements.

Optional modules do not attempt a full definition of each of the areas specified. The aim is to identify only requirements which overlap in functionality with, or which have an impact on, electronic records management. This includes issues related to the reliability and authenticity of electronic records and metadata.

Optional modules are included in this consultative draft for:

- Authentication and Encryption
- Document Management
- Hybrid and Physical File Management

Modules are planned, and will be released later, for:

- Content Management
- Image Management
- Case Management and Workflow

B. 1: AUTHENTICATION AND ENCRYPTION

Electronic signatures

B.1.1 (M) The RKS must be capable of configuration to select the extent to which information about the authentication process is routinely stored, including levels that:

- retain the fact of successful authentication only with the record
- retain information about the authentication process with the record
- retain all authentication data, including signatures, with the record.

B.1.2 (M) The RKS must be able to retain the fact that an electronic signature has been verified as authentic, with the electronic record with which the signature is associated.

B.1.3 (M) The RKS must be able to retain and preserve information about the process of verification for an electronic signature, including either or both:

- the Certification Authority with which the signature has been validated
- the date and time of validation.

B.1.4 (M) The RKS must be able to store 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.1.5 (M) The RKS must be capable of interfacing with electronic signature technologies, so that information about the authentication process is captured automatically.

B.1.6 (M) The RKS must be capable of interfacing with UN approved electronic signature technologies.

B.1.7 (M) The RKS must be capable of checking the validity of a digital signature at the time of creation of the record.

B.1.8 (M) The RKS must be capable of demonstrating the continued integrity of an electronically signed record, even though allowable changes have been made to the metadata for that record (but not to the content).

B.1.9 (HD) The RKS should be capable of applying an electronic signature to a record, or folder of records, during the process of export, in such a way that the signature can be validated externally to the RKS.

Electronic watermarks

B.1.10 (M) The RKS must be capable of storing records bearing electronic watermarks, and of retaining information about the watermark with the record.

B.1.11 (HD) The RKS should be capable of applying an electronic watermark to a record, or group of records, during the process of export from the RKS ,without any subsequent loss of access in a receiving system which is different from the RKS.

Encryption

B.1.12 (M) The RKS must be able to ensure the capture of, and create, 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.

B.1.13 (M) The RKS must be capable of allowing encryption to be removed when a record is captured or created directly from a software application.

B.1.14 (M) Where an electronic record has been sent or received in encrypted form by a software application which interfaces with the RKS, the RKS 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.1.15 (M) Where an electronic record in encrypted form has been transmitted by or captured from, a software application which interfaces with the RKS, the RKS must be able to keep as metadata with that record:

- the fact of encrypted transmission or capture
- the type of algorithm

- the level of encryption used.

B.2: DOCUMENT MANAGEMENT

B.2.1 (M) The EDRMS must either provide document management facilities as an integral part of the system or must be capable of integration with one or both of:

- an electronic document management system capable of passing management
- control of documents within its own filestore(s) to an RKS at time of creation;

- an electronic document management system capable of transferring created documents as records to an RKS directly from the EDM system.

B.2.2 (M) Where an RKS is integrated with an EDMS, it must in principle be capable of integration with new EDM systems and new versions of existing integrated EDMS.

B.2.3 (M) The EDRMS must enable a newly created document to be captured and created by the EDRMS in one operation.

B.2.4 (M) The EDRMS must enable a newly created document to be captured and not created by the EDRMS.

B.2.5 (M) The EDRMS must enable a document already existing in the document management environment or capability to be created as a record in one operation.

B.2.6 (M) The EDRMS must support the creation of versions of electronic documents which are closely bound together, and must manage version control to support progressive drafting and ensure continual integrity of the document as a whole.

B.2.7 (M) Where more than one version of the document has been created, the EDRMS product set must support the ability to create:

- the most recent version
- one specified version only
- all existing versions, and hold all of these as a single electronic record.

B.2.8 (M) The EDRMS product set must be capable of allowing versions of a document to be created, as part of drafting process, without automatically creating a new record on each occasion.

B.2.9 (M) The EDRMS product set must support the ability to define different templates for electronic documents, and the allocation of different metadata elements sets for each template. Examples of distinct types are:

- pre-defined forms
- report layouts
- standard letter formats

B.2.10 (M) The EDRMS product set must be capable of configuring the mapping of

electronic document metadata to electronic record metadata, to ensure that an electronic record always possesses correct and authentic metadata as defined by the accompanying records management metadata standard and in accordance with RKS functional requirements.

B.2.11 (M) The EDRMS product set must allow metadata to be acquired from the user during the process of creation.

B.2.12 (M) When declaring a record, the EDRMS product set must give precedence to the process of capturing metadata in accordance with RKS functional requirements above metadata from the document management environment or capability, where any potential conflict arises.

B.2.13 (M) The EDRMS product set must ensure that any metadata captured in the document management environment or capability, that will be carried over into records management metadata, is managed in accordance with RKS functional requirements to ensure authenticity.

B.2.14 (M) When declaring a record, the EDRMS product set must give precedence to the access controls for the record in accordance with RKS functional requirements above access controls applying in the document management environment or capability, where any potential conflict arises.

B.2.15 (M) The EDRMS product set must not allow a concept of ownership which, within the document management environment or capability gives rights that must not be allowed within the records management environment or capability, to apply to a created record[54].

B.2.16 (M) The EDRMS product set must not allow a created record to be checked out, where this implies any capability to amend/alter the record content in any way.

B.2.17 (HD) The EDRMS product set should be capable of managing documents and records within the same class and folder structure[55].

B.2.18 (M) Where the EDRMS product set is capable of managing documents and records within the same class and folder structure, it must make a clear and immediately visible distinction between documents created as records and those that are not.

B.2.19 (M) Where the EDRMS product set is capable of managing documents and records within the same class and folder structure, it must provide options for:

- automatically declaring all uncreated documents in a specified folder or folders as records;

---

[54] *For example, rights of edit on document content, rights of edit on certain metadata elements, rights of deletion*

[55] *That is, documents that have been created/captured as records, and documents that have not been declared as records within the same folder*

- automatically deleting all uncreated documents in a specified folder or folders;

- automatically deleting all uncreated documents in a specified folder or folders that are older than a specified period of time.

B.2.20 (M) Where the EDRMS product set is capable of managing documents and records within the same class and folder structure, it must:

- provide a notification, within the disposal management mechanism, where uncreated documents exist within a folder to be exported, and enable them to be created as records;

- export only the records within that folder;

- in a transfer process, automatically destroy any remaining documents when the records are destroyed following confirmation of successful export.

B.2.21 (HD) The EDRMS product set should support a personal workspace for each user, used for storing drafts of document which are not yet (and which may never be) created as records[56].

B.3: HYBRID AND PHYSICAL FOLDER MANAGEMENT

B.3.1 (M) The RKS must support the management of physical folders in a manner which is closely integrated with the management of electronic folders and electronic records.

Physical folders

B.3.2 (M) The RKS must enable the definition of physical folders and parts, and the allocation of physical folders to a class.

B.3.3 (M) The RKS must enable the definition of hybrid folders and hybrid parts, which are part physical and part electronic, and the allocation of a hybrid folder to a class.

B.3.4 (M) The RKS must support the use of metadata for physical and hybrid folders, and the inheritance of metadata from a class consistent with inheritance by an electronic folder.

B.3.5 (M) The RKS must support the capture and presentation of metadata for physical and hybrid folders as set out in the accompanying metadata standard for records management.

---

[56] *Such a personal workspace may also distinguish between private and public documents, neither of which are records*

B.3.6 (M) The RKS must allow a different metadata element set to be configured for physical folders than that for electronic folders; so that physical folder metadata can include information on the location of the folder; and the RKS must record the fact of changes to such metadata in the audit trail.

B.3.7 (M) The RKS must allow both the physical and electronic folder associated together as a hybrid to use the same folder title or file plan id, but with an added indication one is a paper and the other an electronic folder.

B.3.8 (M) The RKS must ensure that creation of a new part within either of an electronic or a physical folder which are associated together as a hybrid, automatically creates a new part in the companion electronic or physical folder.

Markers

B.3.9 (M) The RKS must support the creation of markers – that is, a metadata profile of a physical record held outside the RKS – and their allocation to electronic folders[57].

B.3.10 (M) The RKS 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 their physical location.

B.3.11 (M) The RKS must allow markers to denote different types of physical record; examples include:

- information about a large volume paper record, map or plan
- information about a database
- information about a video.

B.3.12 (M) The RKS must be able to associate a marker with one or more electronic folders.

B.3.13 (M) The RKS must be able to record the fact of a change made to metadata about a marker in the audit trail.

Retrieval and access control

B.3.14 (M) The RKS must be able to search for and retrieve markers and physical folders, and electronic records and folders, by a single integrated search.

B.3.15 (M) The RKS must ensure that retrieval of a complete electronic folder also retrieves all markers associated with that folder.

---

[57] *In the model used by these requirements, it is **not** envisaged that markers will be allocated to physical folders, i.e. listing the individual contents of physical files is not within scope*

B.3.16 (M) The RKS must ensure that retrieval of an electronic folder or physical folder which is part of a hybrid folder, also retrieves the companion electronic or physical folder associated with the hybrid.

B.3.17 (M) The RKS must ensure that (within the RKS) both electronic and physical folders of a hybrid folder are allocated the same access controls..

B.3.18 (M) The RKS must be able to control user access to metadata about markers and physical folders, (within the RKS) consistent with access controls for electronic records and folders[58]

Tracking and circulation

B.3.19 (HD) The RKS should support the production of barcodes for locating and tracking physical folders and parts.

B.3.20 (HD) The RKS should support check-out and check-in facilities for physical folders and parts, recording a specific user or location to which a physical folder or part is checked-out, and the date on which this occurred, and displaying this information where the physical folder is retrieved by another user, unless restricted by access controls or protective marking.

B.3.21 (HD) The RKS should support a bring forward facility for physical folders and parts, enabling a user to enter a bring forward or reserve date for a physical folder or part, and generating a consequent message for transmission to the current holder of that folder or another authorized user, according to configuration.

B.3.22 (HD) The RKS should support a bring forward facility for electronic folders, enabling a user to enter a bring forward date for an electronic folder, so that the user receives an automatic reminder bringing the electronic folder to attention at the date to be brought forward.

B.3.23 (D) The RKS may support an ordering facility, enabling a user to request a physical folder located with another user or a storage facility.

Disposal

B.3.24 (M) The RKS must support the allocation of a disposal schedule to a physical folder.

B.3.25 (M) The RKS must ensure the same disposal schedule is always applied to both of the electronic and physical folders associated together as a hybrid folder[59].

---

[58] *Bearing in mind the requirement at A.5.52*

[59] *This may be achieved by inheritance from the hybrid folder.*

B.3.26 (M) The RKS must ensure that any disposal actions on a hybrid folder are explicitly carried out on both the electronic and physical folder (within the RKS) associated as a hybrid, at the same time and in the same manner.

B.3.27 (M) The RKS must ensure that any review decisions made on an electronic folder that is associated as a hybrid with a physical folder, are also applied (within the RKS) to the physical folder.

B.3.28 (M) The RKS must be able to export physical folders, and retain all their associations with classes and electronic folders associated as a hybrid, once exported.

B.3.29 (M) The RKS must be able to export markers, and retain all their associations with electronic folders and other electronic records, once exported.

B.3.30 (M) Where an electronic folder containing markers is to be destroyed or transferred, the RKS must ensure that the markers are destroyed at the same time as the contents of the electronic folder.

B.3.31 (HD) Where a hybrid folder is to be destroyed, exported or transferred, the RKS should require an authorized user to confirm that the physical folder of the hybrid has been destroyed, ‘exported’ or transferred before processing the electronic folder.

B.3.32 (HD) Where the RKS supports the maintenance of a minimum metadata ‘stub’ to denote the former existence of a folder, the RKS must ensure that minimum metadata is maintained for a physical folder that has been destroyed, and for both electronic and physical folders in a hybrid folder.