Date: 4th September 2007

Author: MoReq2 Team

MoReq2 Draft 2

THIS DRAFT

This draft is substantially complete except for:

- section 11.7 - Long Term Preservation and Technology Obsolescence, which has not been fully revised;
- chapter 12 - Metadata Requirements;
- most of the Appendices.

There are still some areas that we will be dealing with at a later stage. In later drafts we will;

- Make the use of "overview" and "introduction" sections in chapters and sections more consistent.
- Add appendices.
- Add any missing cross-references.
- Make the capitalisation and other punctuation consistent.
- Make sure all the standards listed in Appendix 7.5 are referred to.
- Try to re-sequence some of the requirements to make the flow more logical within sections.
- Renumber all the sections and requirements. The numbering will adopt the same structure as the numbering in MoReq; for example, the second requirement in section 4.1 will be numbered "4.1.2". All the <ID> numbers will be replaced.

Please do not submit comments about these issues!

This draft contains some major changes. The most important changes are highlighted. It also shows, for the first time, the "testability" for each requirement. See <ID4551> in section 1.11 for details.

Contents

1 Introduction

1.1 Background

ID	Text
44	**Introduction**
2048	**Background**
46	The need for a comprehensive specification of requirements for electronic records management was first articulated by the DLM-Forum in 1996 as one of its ten action points. Subsequently, the European Commission commissioned the development of a model specification for electronic records management systems (ERMS). The result, MoReq, the Model Requirements for the management of electronic records, was published in 2001.
3300	Footnote DLM is an acronym for "Document Lifecycle Management" (it formerly was an acronym for the French "Données Lisibles par Machine," in English: "machine-readable data.") The DLM-Forum is based on the conclusions of the European Council (94/C 235/03) of 17 June 1994 concerning greater cooperation in the field of archives.
3301	Footnote MoReq is available from <insert permanent url here>; it is also published in paper form, with ISBN 92-894-1290-9.
3287	MoReq was widely used in throughout the European Union and beyond. However, there was no maintenance regime for MoReq; and there was no scheme to test software compliance against the MoReq specification.
47	Demand for both updates to MoReq and a compliance testing scheme grew. The DLM Forum entered into discussions with the European Commission. This culminated in the Commission's Secretariat-General (Directorate B e-Domec and archives) launching an open competition for the development of this document, MoReq2, in 2006. Development was carried out during 2007 by a small team of specialist consultants from Serco Consulting (formerly Cornwell Management Consultants plc), supported by an Editorial Board of experts drawn from several countries, and numerous volunteer reviewers from both the private and public sectors.
48	Appendix 2 contains further detail on the methodology used, and Appendix 4 acknowledges the contributions of the review panel members who kindly volunteered their time, intellect, and experience.

1.2 Relationship between MoReq and MoReq2

ID	Text
3288	**Relationship between MoReq and MoReq2**
3289	MoReq2 is intended to replace MoReq.
3290	The specification for MoReq2 is contained in the "Scoping Report" for MoReq2. It describes the aims of MoReq2 as follows:
3291	Footnote Insert a persistent URL here when known
3292	"The overall aims for the MoReq2 development are to develop extended functional requirements within a European context, and to support a compliance scheme by: • Strengthening from MoReq what have in the interim become key areas and covering important new areas of requirements with clarity; • Ensuring that the functional requirements are testable and developing test materials to enable products to be tested for compliance with the requirements; • Making the requirements modular to assist application in the various environments in which they will be used."

ID	Text
3288	**Relationship between MoReq and MoReq2**
3293	"To provide compatibility, MoReq2 is to be an evolutionary update to the original MoReq, not a radically different product."
3294	The concept of "evolutionary upgrade" is key. MoReq2 is almost entirely compatible with MoReq (minor incompatibilities are clearly indicated); it is based on the same concepts, and as a document it uses a similar structure.

1.3 Purpose and Scope of this Specification

ID	Text
49	**Purpose and Scope of this Specification**
50	This specification is the second version of the Model Requirements for the Management of Electronic Records. (MoReq2). It focuses mainly on the functional requirements for the management of electronic records by an Electronic Records Management System (ERMS).
51	This specification is written to be equally applicable to public and private sector organisations which wish to introduce an ERMS, or which wish to assess the ERMS capability they currently have in place.
52	While the specification focuses on functional requirements, it recognises that non-functional attributes are central to the success of an ERMS, as with any information system. However, these non-functional attributes vary enormously between environments. Accordingly, they are identified but described only in outline.
53	Other closely-related requirements, such as document management and the electronic management of physical records (e.g. paper files and microfilm) are also addressed, but in less detail. Related issues such as digitisation and other means of creating electronic records are outside the scope of this specification. Similarly, it makes no attempt to cover the practical implementation of an ERMS.
54	This specification is written with the assumption that ERMS users include not only administrators, records managers or archivists, but also general office and operational staff who use ERMS as part of their everyday work while creating, receiving and retrieving records.
55	As this specification contains "model" requirements, it is designed to be entirely generic. It does not consider any platform-specific or sector-specific issues. Because it is modular, user communities can add to it additional functionality specific to their own business requirements (see section <1.6> and <Appendix 3> for guidance on using and customising this specification).

1.4 What is an ERMS?

ID	Text
56	**What is an ERMS?**
57	The management of electronic records is complex, requiring a large range of functionality to be implemented well. Typically, a system to meet these needs - an ERMS - requires specialised software, though increasingly records management functionality is being built into operating system software and other applications. Specialist software may consist of a single package, a number of integrated packages, custom-designed software or some combination; and in all cases, there will be a need for complementary manual procedures and management policies. The nature of an ERMS will vary from organisation to organisation. This specification makes no assumption about the nature of individual ERMS solutions. Users of this specification will need to determine how the functionality of an ERMS can be implemented to meet their requirements.

ID	Text
56	**What is an ERMS?**
4180	MoReq2 is written primarily to describe application software that is designed expressly to manage records. However, it may also be used as a statement of outcomes together constituting electronic records management. Thus the statements in MoReq2 saying "The ERMS must or should…" may also be read as shorthand for "The using organisation's application system and/or the supplier platform must or should…" Readers of MoReq2 need to decide which requirements are necessary in their environment.
4461	The full set of MoReq2 requirements may be appropriate for integrated application systems. However, a subset may be more appropriate in the situation, for example, where records management features are needed as part of a case management or line of business application.
4182	The optional modules 10.5 Workflow and 10.6 Case Management, specifically apply to line of business applications. However much of the functionality described in the requirements throughout MoReq2 can also be applicable and should be considered when implementing these business systems.

1.5 For what can this specification be used?

ID	Text
58	**For what can this specification be used?**
59	The MoReq2 specification is intended to be used: • **by potential ERMS users:** as a basis for preparing an invitation to tender; • **by ERMS users:** as a basis for auditing or checking an existing ERMS; • **by training organisations:** as a reference document for preparing records management training, and as course material; • **by academic institutions:** as a teaching resource; • **by ERMS suppliers and developers:** to guide product development by highlighting functionality required; • **by record management service providers:** to guide the nature of the services to be provided; • **by potential users of outsourced record management services:** as an aid in specifying the services to be procured.
4651	In addition, when used with the testing framework documentation developed in parallel with MoReq2, it is intended to be used: • **by ERMS suppliers and developers:** to test ERMS solutions for MoReq2 compliance; • **by ERMS users:** to test ERMS implementations for MoReq2 compliance.
67	The specification is written with an emphasis on usability. Throughout, the intention has been to develop a specification which is useful in practice.

1.6 Intellectual property rights

ID	Text
4379	**Intellectual property rights**
4380	All intellectual property rights in MoReq2, including use of the name MoReq2, lie with the European Commission. Accordingly, permission must be given before any chapter zero to MoReq2 is published – see the formal notice on the title page. Applications for permission should be addressed to <dlm-forum@cec.eu.int?>.

1.7 Emphasis and Limitations of this Specification

ID	Text
68	**Emphasis and Limitations of this Specification**

ID	Text
68	**Emphasis and Limitations of this Specification**
69	The MoReq2 specification is designed explicitly with pragmatism and usability in mind. It is primarily intended to serve as a practical tool in helping organisations meet their business needs for the management of both computer-based and paper-based records. While its development has taken traditional archival science and records management disciplines into account, these have been interpreted in a manner appropriate to electronic environments. Thus, MoReq was developed with the needs of managers of both electronic and physical records in mind.
70	The requirements in MoReq2 should, if implemented, result in a system which will manage electronic records with the desired levels of confidence and integrity, by combining both the advantages of electronic ways of working with classical records management theory. Examples of this pragmatic approach include the incorporation of requirements for document management, workflow, metadata and other related technologies.

1.8 Considerations for individual Member States

ID	Text
4381	**Considerations for individual Member States**
71	As explained in the section on scope <section 1.x>, this specification attempts to cover a wide range of requirements - for different countries, in different industries and with different types of records. The wide scope is intentional; but it leads to a significant limitation, namely that this single specification cannot represent a requirement which precisely maps onto existing requirements without modification. Different countries have their differing traditions, views and regulatory demands for managing records. In some cases these will have to be taken into account when applying this Model Requirements Specification, especially when using it to specify a new system. For this reason, MoReq2 allows for individual European Union countries to add a "national chapter", or "chapter zero," that sets out national requirements such as.
3868	• Translations of key terminology and key concepts; • National legislative and regulatory requirements; • National standards and guidance on accessibility; • Potentially, other national requirements; • National resources for further information.
72	Although MoReq2 covers a wide range of types of records, it is important to understand that ERMS solutions address mainly records that are often referred to as "unstructured" records <insert footnote>. In simple terms, unstructured records are those that contain information presented in a form primarily intended to be used by human users. Examples of unstructured records are letters, memoranda, e-mail messages, pictures, photocopies, scanned images, audio recordings and video recordings. Structured records by contrast contain information in a form intended to be used primarily by computer applications (examples include accounting system records, manufacturing scheduling system records, and air traffic control system records). While an ERMS can, in principle be used to store such structured records, it rarely is; in the vast majority of situations, structured data is stored under the management of a data processing application (in the examples above these might be a general ledger system, a manufacturing scheduling system, and an air traffic control system). ERMS solutions are used almost universally to store and manage unstructured records. The instances in which an ERMS is used for structured records occur mainly in case management environments - see section <10.6>.
3869	<Footnote>It can be held that all properly managed electronic records are structured, as they all are linked to metadata, audit trail data etc. in a structured manner. On this basis it would be more accurate to refer to unstructured records as "records containing unstructured content"; however, this usage is not common and so is not adopted in MoReq2.

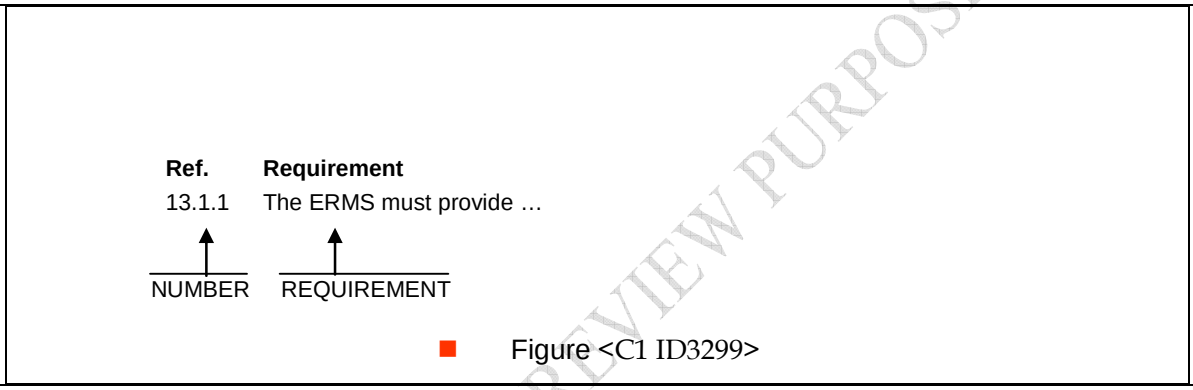
ID	Text
4381	**Considerations for individual Member States**
3297	MoReq2 does not cover the practical aspects of the management of records. Intentionally, the specification addresses only the capabilities required for the management of electronic records by software. The specification avoids discussion of records management philosophy, archival theory, decision taking, management control etc.; these issues are well covered in other literature, some of which is listed in Appendix 1. As a particular example, the specification mentions in several places that certain functions must be limited to administrative roles. This is not to say that administrative roles have to take policy decisions, merely that they must be the only users empowered by the organisation to execute them through the ERMS.
4183	It is important to note that records management and policy must be integrated with the organisation's business and technical requirements and that an administrative role can only implement, from a records management and system perspective, decisions taken by more senior management.
73	Finally, this specification is intentionally user-centric; it uses, as far as possible, the type of terminology commonly used by those working with electronic records. For example, the specification describes electronic files as "containing" records, for ease of understanding, even though electronic files strictly do not contain anything. See section <2.2> for further details.

1.9 Using this Specification

ID	Text
74	**Using this Specification**
75	The requirements in this specification are intended to serve only as a model. They are not prescriptive for all possible ERMS implementations; some requirements will not apply in some environments. Different business sectors, different scales, different organisation types and other factors will also introduce additional specific requirements.
3298	As a result, **this specification must be customised before use for procurement purposes**. The customisation for procurement should: • add or remove requirements as specifically required by the organisation; • adjust requirements that can be made more specific (for example, requirements that specify one of several possible outcomes can be changed to specify a single required outcome; or requirements for volumes and performance) • include details specific to the organisation, such as the software environment; • indicate clearly which requirements are: o unchanged from MoReq2, o new, o deleted, o adjusted.
76	This specification has been prepared so that it can be used in paper or electronic form. It has been prepared using Microsoft Word 2003, and is published in <insert Word format details here when known>. Use in electronic form has a number of benefits; details are given in Appendix 3.

1.10 Organisation of this Specification

ID	Text
77	**Organisation of this Specification**
78	The specification is organised into chapters which are divided into sections.
79	The next chapter (chapter 2) provides an overview of some of the key requirements, starting with terminology which is central to this specification.

ID	Text
77	**Organisation of this Specification**
80	Chapters 3 to 10 contain the ERMS functional requirements in detail. Each chapter contains a logical grouping of functional requirements. However, given the nature of the subject matter there is inevitably some overlap between chapters.
3737	Chapter 10 is divided into several sections, each of which represents requirements for an optional module of an ERMS. Some of these sections (e.g. the section on distributed systems) will be essential for some organisations, but unnecessary for others.
3738	Chapter 11 contains non-functional requirements.
3739	In response to demand from many sources, the DLM Forum is planning to implement a MoReq2 Testing Framework. The structure of MoReq2 is designed to support this framework, e.g. each section of chapter 10 represents one optional test module. For more detail on the MoReq2 Testing Framework see <insert persistent url here>.
81	Each requirement is presented in a standard format, as illustrated below.
82	The requirements are presented in the form of tables, with one requirement per table row. This is illustrated below.
3299	 Figure <C1 ID3299>
103	Each requirement bears a number, and each is expressed in natural language.

1.11 Compliance Testing

ID	Text
3554	**Compliance testing**
4551	**Testability**
3555	Each requirement is followed by an attribute called "testable". This indicates whether it will be possible to test compliance with the requirement. Possible values of the "testable" attribute are described below, with examples: • **Y - The requirement can be tested formally.** An example is *"The ERMS must allow at least three hierarchical levels in the classification scheme"*. This can be tested by attempting to set up a hierarchy with three levels. • **N - The requirement cannot be tested formally.** An example is *"The ERMS must support the organisation's business classification scheme"*. There is no way to test this in the general case. • **P - The requirement can be tested but the coverage of the test is partial, and/or it is possible that lack of compliance can be discovered.** An example is *"the ERMS should not limit the number of levels in the hierarchy."* There is no way, formally, to test for the absence of a limit. However, the requirement is considered testable with partial coverage, for example by testing for a large number of levels; and during the testing it is possible that a limitation on the number of levels might be noticed, indicating that the ERMS does not comply with the requirement.
4552	**Systems beyond the ERMS**
4652	This specification is accompanied by the MoReq2 Testing Framework. The framework provides documentation that allows the compliance of an ERMS against MoReq2 to be tested.

ID	Text
3554	**Compliance testing**
4553	Several MoReq2 requirements rely on hardware and software that is beyond the boundaries of the ERMS. For example, MoReq2 includes: • requirements about e-mail integration that rely on features of e-mail software; • scalability and integrity requirements that rely on features of database management software; • scanning requirements that rely on scanning hardware.
4554	Clearly it is not possible to test any ERMS with all possible hardware and software that might be used. Therefore, and as a matter of definition, such requirements will be tested with a combination of software and hardware specified by the ERMS supplier. The resulting compliance test certificate will specify the software and hardware that has been used for the test; compliance will extend to that environment only. Potential users of the ERMS wishing to know the compliance with any other software and/or hardware will need to assess it on a case by case basis.
104	Chapter 12 identifies requirements for managing metadata; definitions of the metadata elements needed to support MoReq2 are in Appendix 9.
105	Chapter 13 contains a formal reference model of ERMS as understood in this specification. This model can be used to understand key aspects of the specification, such as formal definitions of terms (e.g. class, sub-file, volume) and the relationships which exist between them (e.g. "what can be stored in an electronic file?").
106	The Appendices contain details of reference documents, administrative and other information.

1.12 Mandatory and Desirable Requirements

ID	Text
107	**Mandatory and Desirable Requirements**
108	MoReq2 contains both mandatory and optional requirements. This level of mandation is indicated as follows • the word "must" indicates that a requirement is mandatory; • the word "should" indicates that a requirement is desirable.
3681	In all cases, the level of mandation is dependent on its context. So, for example, a mandatory requirement in an optional module is mandatory only in the context of that optional module.

1.13 Comments on this Specification

ID	Text
111	**Comments on this Specification**
112	Please send any comments and observations on this specification to: <insert e-mail address when known>

2 Overview of ERMS Requirements

ID	Text
114	**2 Overview of ERMS Requirements**
115	This chapter starts by defining some key terms (section 2.1). This is followed by a narrative description of some key concepts (section 2.2), and an entity-relationship diagram of the model on which this specification is based (section 2.3).

2.1 Key Terminology

ID	Text
116	**2.1 Key Terminology**

ID	Text
116	**2.1 Key Terminology**
118	MoReq2 requires certain terms to have precise meanings. Wherever possible, the meanings align with common usage, or usage generally agreed within the records management community. However, in some cases the usage is specific to MoReq2. All the terms are defined in the Glossary (section 13.1); selected key definitions from the Glossary are reproduced here for ease of reference.
119	In this Glossary, terms in *italics* are defined in the Glossary, section 13.1.
120	**capture**
4556	(1) The act of recording or saving a particular instantiation of a digital object (source: InterPares 2 Project Terminology Database).
4557	(2) Saving information in a computer system.
121	Note: in the context of MoReq2, capturing *records* is used to mean all of the processes involved in getting a record into an ERMS, namely registration, classification, addition of metadata, and freezing the contents. The term is used more generally to mean inputting to the ERMS and storing other information such as metadata values.
3726	**case file**
3727	A file relating to one or more transactions performed in a structured or partly-structured way.
3731	Source: adapted from PRO Functional Specification of "electronic file" (Appendix 1 reference [2]).
3730	Note: there is no universally-accepted definition of these terms, nor of the distinction between case files and the other kinds of files often managed by an ERMS. The following is therefore developed for, and intended to facilitate the understanding of MoReq2; its applicability in other situations is not guaranteed.
3729	Note: the records in the file may be structured or unstructured. The key distinguishing characteristic of case files is that they result from processes which are at least partly structured. Examples include files about: • applications for permits, etc.; • enquiries about a routine service; • investigation of an incident; • regulatory monitoring.
3728	Note: typically, other characteristics of case files are that they often: • feature a predictable structure for their content; • are numerous; • are structured or partly structured; • are used and managed within a known and predetermined process; • need to be retained for specific periods, as a result of legislation or regulation; • can be opened and closed by practitioners, end-users or data processing systems without the need for management approval.
122	**class**
123	(In this specification only) The portion of a hierarchy represented by a line running from any point in the *classification scheme* hierarchy to all the files below it.
124	Note: this can correspond, in classical terminology, to a "primary class", "group" or "series" (or sub-class, sub-group, sub-series etc.) at any level in the classification scheme.
125	**classification**
126	In records management, the systematic identification and arrangement of business activities and/or *records* into categories according to logically structured conventions, methods, and procedural rules represented in a classification system.
127	Source: ISO 15489 (see Appendix 1 reference [9]).
128	**classification scheme**
129	See classification.

ID	Text
116	**2.1 Key Terminology**
130	Source: definition of "Classification System" in ISO 15489 (see Appendix 1 reference [9])
131	Note: a classification scheme is typically represented as a hierarchy.
3339	**component**
3340	A distinct byte stream that, alone or with other byte streams, makes up a *record* or *document*.
3341	Note: This term is not in general use.
3342	Note: The phrase "distinct byte stream" is used to describe what is usually called a "file" in information technology. The word "file" is avoided here to prevent confusion with the records management meaning of "file". The key concept here is that a "component" is an integral part of the content of a record, despite the fact that it can be handled and managed separately by an operating system.
3343	Note: The phrase "distinct byte stream" is used to describe what is usually called a "file" in information technology; the word "file" is avoided here to prevent confusion with the records management meaning of "file". The key concept is that a "component" is an integral part of the content of a record, despite the fact that it can be handled and managed separately. Note: Examples of components include: • An html document and JPEG images that make up a web page; • A word processing document and a spreadsheet, where the record consists of the word processing document that contains an embedded link (a hyperlink) to the spreadsheet.
3344	Note: components have to be distinct, i.e. separate from each other. If a word processed document contains an embedded spreadsheet (as opposed to an embedded link to a spreadsheet) then the spreadsheet is not considered to be a component; in this case, the word processed document complete with its embedded spreadsheet is a record made up of one component.
4558	Note: an e-mail message with attachments may be regarded as one component, as several components, or as several records, depending on the format in which it is stored. • If the message is stored in a format that includes the body and all its attachments, then there is only one component. • If the attachments are stored separately from, and linked internally to, the body of the e-mail message, then each attachment and the body of the message is a component. • If the attachments are stored separately from the body of the e-mail message but they are not linked internally, then each attachment and the body of the message is a separate record; good practice suggest that these records should be linked to each other manually.
132	**document** (noun)
133	Recorded information or object which can be treated as a unit.
134	Source: ISO 15489 (international standard; see Appendix 1 reference [9]).
135	Note: a document may be on paper, microform, magnetic or any other electronic medium. It may include any combination of text, data, graphics, sound, moving pictures or any other forms of information. A single document may consist of one or several objects.
136	Note: documents differ from *records* in several important respects. MoReq2 uses the term document to mean information that is not a record.
141	**electronic record**
142	A *record* which is in *electronic* form.
143	Note: it can be in electronic form as a result of having been created by application software or as a result of digitisation, e.g. by scanning.
144	**ERMS**
145	Electronic Record Management System.
146	Note: ERMS differ from *EDMS* in several important respects. See section 10.3 for more details.
147	**metadata**

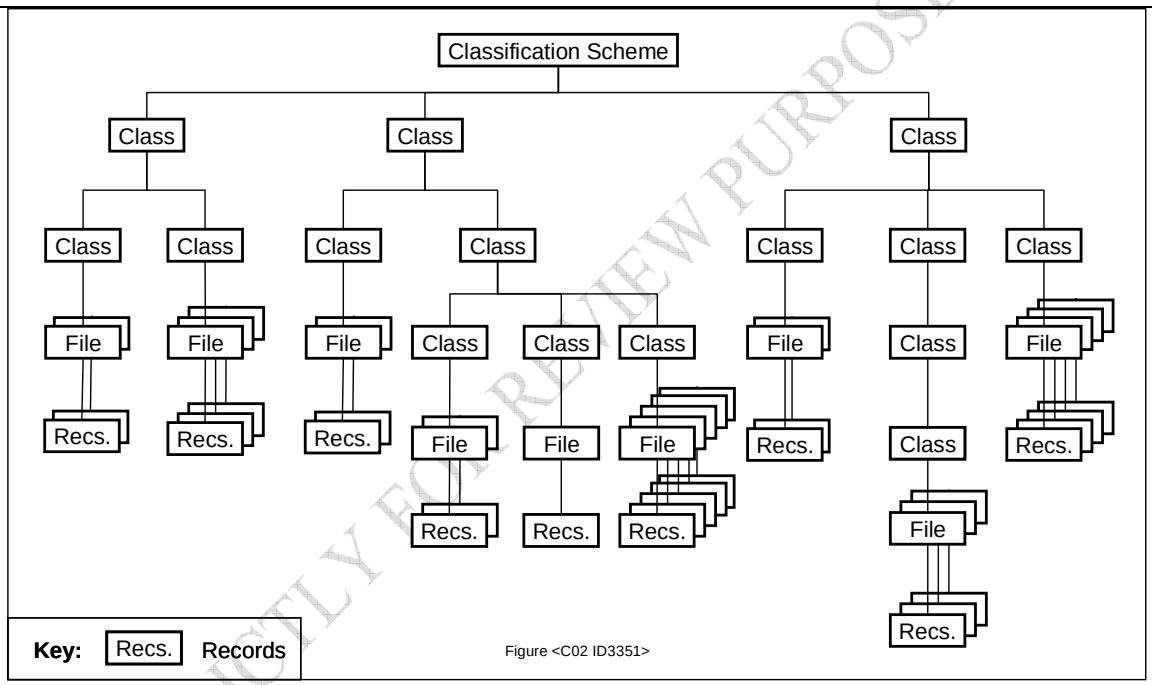
ID	Text
116	**2.1 Key Terminology**
148	(In the context of records management) Data describing context, content and structure of records and their management through time.
149	Source: ISO 15489 (see Appendix 1 reference [9]).
150	Note: the distinction between data and its metadata can be unclear. For example, it is usually clear that the essential indexing data for a record (title, date etc.) is part of that record's metadata. However, the audit trail for a record, or the Retention and Disposition Schedule for a record, can validly be considered to be either data or metadata, depending on the context. Different types of metadata can be defined, for example, for indexing, for preservation, for rendering etc. These details of metadata usage are beyond the scope of MoReq2.
151	**record** (noun)
152	Information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business.
153	Source: ISO 15489 (see Appendix 1 reference [9]).
154	Note: local national definitions may also apply.
155	Note: a record may incorporate one or several *documents* (e.g. when one document has attachments), and may be on any medium in any format. In addition to the content of the document(s), a record should include contextual information and, if applicable, structural information (i.e. information which describes the components of the record). A key feature of a record is that it cannot be changed.
4641	Note: both *electronic records* and *physical records* can be managed by an *ERMS*.
3346	**sub-file**
3347	Intellectual subdivision of a file.
3348	Note: Sub-files are usually used in case file management environments. Typically, each sub-file is named, and each sub-file is used to store a specified kind or kinds of records, such as "invoices", "assessments" or "correspondence".
156	**volume**
157	A subdivision of a *file*.
158	Source: definition of "part" in PRO Functional Specification (Appendix 1 reference [2]).
159	Note: the subdivisions are created to improve manageability of the file contents by creating units which are not too large to manage successfully. The subdivisions are mechanical (e.g. based on number of records or ranges of numbers or time spans) rather than intellectual.

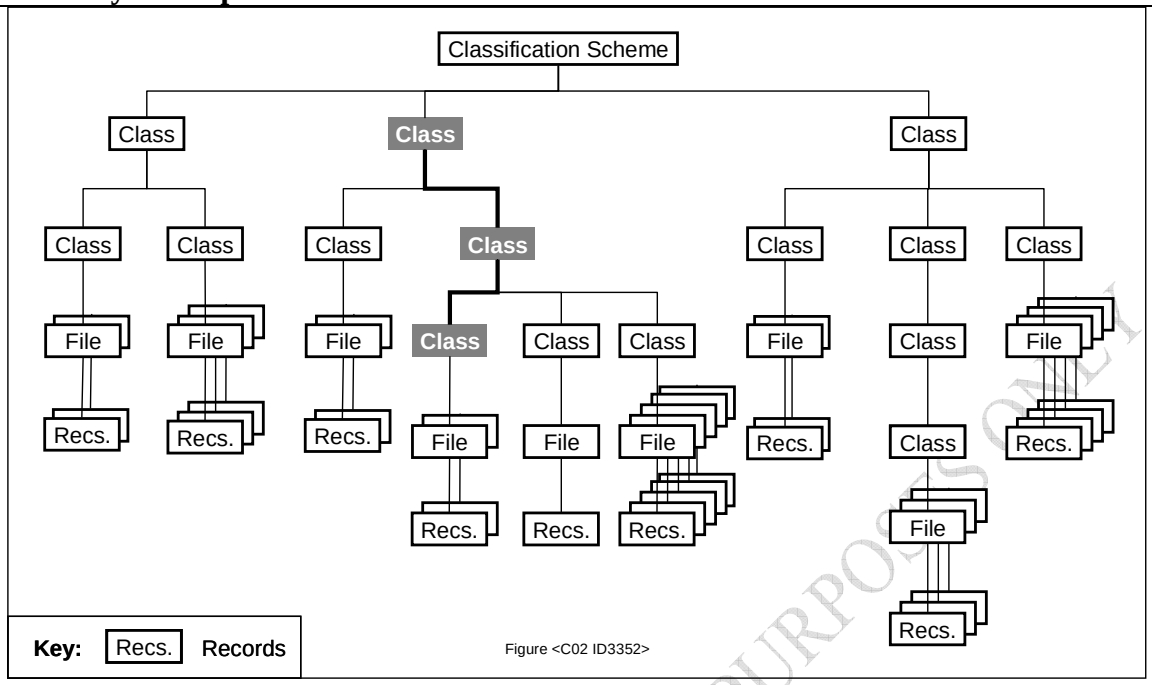
2.2 Key Concepts

ID	Text
160	**2.2 Key Concepts**
161	• The key concepts required to understand this specification are: • record and electronic record; • authoritative record; • electronic file, sub-file and volume; • classification scheme; • class; • ERMS; • capturing records; • user roles.
169	**Record and electronic record**

ID	Text
160	**2.2 Key Concepts**
170	The DLM Forum Guidelines (Appendix 1 reference [6] section 2.4) suggest that records can be viewed as consisting of: • content; • structure; • context; • presentation.
175	The content is present in one or more physical and/or electronic documents which convey the message of the record. These are stored in such a way as to allow future users to understand them and their context. This implies that a record contains, in addition to the content of its document(s), information about the document's context and structure. The presentation depends on a combination of the records contents, structure and (in the case of electronic records) the software used to render it.
176	In the world of physical records, the vast majority of records are on paper and are included in files, physically constituted of one or more volumes of records inserted within paper folders. Procedural controls should prevent users from changing the records, or their positions within the file.
177	Similar concepts apply to electronic records. A record is constituted of one or more electronic documents. These documents can be word processing documents, e-mail messages, spreadsheets, moving or still images, audio files or any other type of digital object. The documents become records when they are set aside, that is, "captured" into the ERMS. Upon capture, the records are "classified", that is they are assigned codes corresponding to the classification scheme class to which they belong, allowing the ERMS to manage them.
3349	For preservation purposes, it is necessary to appreciate that many electronic records are also made up of several components (the word "component" is used in MoReq2 to avoid the IT word "file", so as to reduce the likelihood of confusion with records management "files"). These components are each objects managed by a computer operating system, and they may be in different formats; but they are all needed together to make up a record. Not all records have more than one component; for example, most word processing documents are made of only one component. An example of a record with several components is a web page with text, graphics and style sheets; it is not unusual for a web page to contain one HTML component, dozens of JPEG image components, and a handful of CSS components.
4382	**Authoritative Records**
4383	ISO 15489 describes an "authoritative record" as being a record that has the characteristics of:
4384	• authenticity; • reliability; • integrity; • usability.
4385	As explained in ISO 15489, the aim of all records management systems should be to ensure that records stored within it are authoritative. Summarising, authoritative records:
4386	• can be proven to be what it purports to be; • can be proven to have been created or sent by the person purported to have created or sent it; • can be proven to have been created or sent at the time purported; • can be depended on because its contents can be trusted as a full and accurate representation of the transactions, activities or facts to which it attests; • is complete and unaltered; • can be located, retrieved, presented and interpreted.

ID	Text
160	**2.2 Key Concepts**
4387	The requirements in MoReq2 are designed to ensure that records stored in a MoReq2-compliant ERMS are authoritative. However, compliance with these requirements alone is not sufficient; the existence of, and compliance with, corporate policies is also required.
178	**Electronic File, Sub-file and Volume**
179	Paper records generally are accumulated in paper files, contained in paper folders. The paper files are aggregated into a structure, or classification scheme. In an ERMS electronic records can be managed as if they are accumulated in electronic files and stored in electronic folders. Strictly, electronic files and folders need not have a real existence; they are virtual, in the sense that they do not really "contain" anything; in fact they consist of the metadata attributes of the records assigned to them. Further, in many cases, there need be no real distinction in the electronic system between file and folder. However, these details are not generally visible to ERMS users; ERMS application software allows users to view and manage folders as if they physically contained the documents logically assigned to the files. This user-centred view is carried forward into this specification. The rest of this specification therefore describes electronic files as "containing" records, for ease of understanding. Note however, that while this specification provides functional requirements for the management of electronic files, it does not prescribe the manner in which the concept of electronic files is implemented.
3350	In some environments it is useful to divide files into sub-files. The division into sub-files is an "intellectual" one; that is it (generally) requires human input to decide into which sub-file a record should be stored. Sub-files are most often used in case processing environments; an example would be the case file for a land sale, which might have sub-files for each of plans, deeds, correspondence with lawyers, and transfer forms.
4197	A sub-file is therefore a division of a file by type of content rather than, as in the case of volume, a division by date of the record. A sub-file can be used to permit the application of a different retention and disposition schedule to a set of records within the file.
180	Regardless of whether sub-files are used or not, files are sometimes divided "mechanically" into file volumes, according to predetermined conventions. The term "mechanically" implies simple adherence to such conventions, which are not based on the intellectual content of the files, but on size, number of records contained in them, or time spans. This practice originated with paper files, in order to restrict them to a manageable size and weight. It can be continued with electronic files, to limit them to a manageable length for appraisal, transfer, or other management purpose. It is especially appropriate for the management of files which are open for long periods and/or which grow to contain a large number of records.
181	While the distinction between files and file volumes is clear, the implications are less clear. This is because the implications of choosing to divide files into volumes vary according to implementation needs. The variation arises as: • some files are closed within a limited time, and so the unit used for management purposes is the file (even though a file may consist of several volumes). Examples are a file of a specific small procurement, or a file of one project; • some files have an unlimited life span (or nearly unlimited life span), and so the unit used for management purposes is the volume. Examples are a file of records about a geographic region, or a file dealing with a subject which is not sensitive to time, such as some policies, or an invoice file where a new volume is started every year.
4388	In relatively rare cases, records may be stored outside of files – by being assigned to a class. This is explained in <section 3.2 <ID4218>.
184	**Classification scheme**

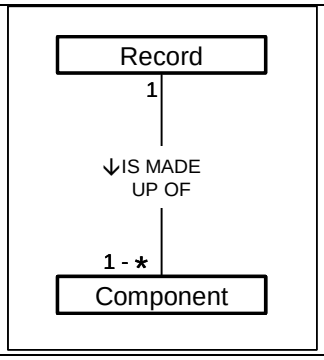
ID	Text
160	**2.2 Key Concepts**
185	Records management aggregates files in a structured manner, and good practice dictates that this structure should reflect business functions. The representation of this aggregation is referred to as a "classification scheme". The classification scheme is commonly a hierarchy, though it may be supported by a thesaurus and may not be hierarchical. The remainder of MoReq2 focuses on the hierarchical view; other approaches are outside the scope of MoReq2, and a hierarchical arrangement is a prerequisite for MoReq2 compliance.
186	Just as files appear to exist even though they are really no more than aggregations of records, so higher levels of the classification scheme hierarchy seem to exist, though they are no more than aggregations of files and/or lower levels. As with files, this specification states requirements for the hierarchy without mandating the manner in which it is implemented.
187	Files can appear at any level of the hierarchy. This is illustrated in the following figure, which represents a fictitious classification scheme, showing its classes and the files allocated to the lowest level classes. This fictitious scheme is much simpler than would be a real classification scheme.
3351	 Figure <C02 ID3351> v2
188	Note that this figure is intended only to show selected possible relationships between levels, files and records. It does not show all possible levels or all possible arrangements.
189	**Class**
190	This specification uses the term "class" to describe the portion of a hierarchy represented by a line running from any point of the hierarchy to all the files below it. The term class therefore corresponds to a "group" or "series" (or sub-group, sub-series etc.) in some texts.
191	In visual terms, a class of a hierarchy corresponds to a branch of a tree. A class may thus contain other classes, just as a series contains sub-series and sub-sub-series. Continuing the above example, the shaded boxes and thick lines in the following diagram are one example of a class.

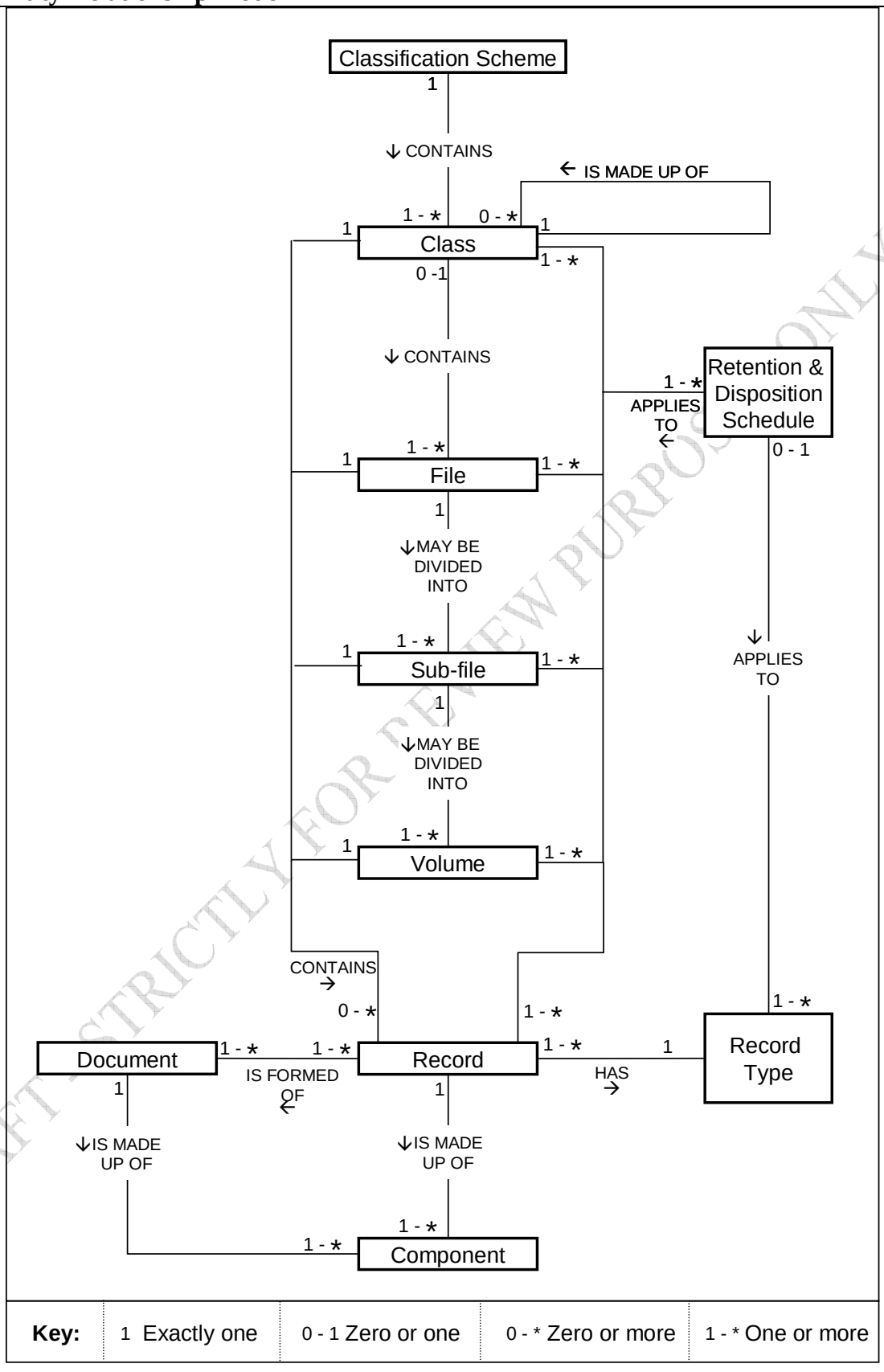
ID	Text
160	**2.2 Key Concepts**
3352	 Figure <C02 ID3352> v2
4639	MoReq2 also uses the term "class" to mean all the files, records etc. assigned to it. This is an intentional simplification, and the distinction between this usage and the above is always clear from the context.
193	**Electronic Record Management System (ERMS)**
194	An ERMS is primarily an application for managing electronic records, though it may also be used to manage physical records. The emphasis of this specification is firmly on the management of electronic records.
195	An ERMS is often closely integrated with an Electronic Document Management System or a business application. Technically, an ERMS manages records, while an EDMS manages documents (which are not records). However, especially when used to support day-to-day working, it can be difficult to separate their functionality. This is explored further in section 10.3 which deals with Document Management issues.
196	**Capturing Records**
197	Documents made or received in the course of business become records when they are set aside, that is, "captured" into the ERMS. During capture, the records are "classified", that is they are assigned codes corresponding to the class to which they belong, allowing the ERMS to manage them; and they are also assigned a unique identifier.

ID	Text
160	**2.2 Key Concepts**
198	In many cases, documents that are set aside, or captured, become records by being bound to a business process, as often happens in a workflow. For example, when an invoice is raised it should automatically cause a record to be captured. In other cases there may be a policy that every document relating to a business matter must become a record, even if it does not formally participate in a business process. In yet other circumstances however, the process of capture will be initiated selectively by a user. Determination of which documents should be captured into a records system should be based on an analysis of the regulatory environment, business and accountability requirements and the risk of not capturing the records. An example is a memorandum in an organisation which deals with policy issues; the organisation may define that only memoranda deemed to be significant will become records (i.e. insignificant memoranda, such as those relating to meeting arrangements, will generally not form records). This specification is intended to cater for any of these scenarios. In other words, MoReq2 describes an office system for general use, not simply a records management system for particular kinds of application or for the exclusive use of archivists or administrators.
199	**User and Administrative Roles**
4389	Different organisations will implement an ERMS differently. For example, a small organisation may implement an ERMS with a single administrator, while a large organisation may need several different administrative positions each with different access permissions. For this reason, it is not helpful to identify specific access profiles in this generic specification; instead, MoReq2 uses the concept of "roles".
200	MoReq2 identifies two kinds of roles: "user roles" and "administrative roles". In practice, most organisations will have more than one person in these roles; and many organisations will define further roles. Example roles with possible access permissions are outlined in the matrix at chapter 13.4.
3697	In brief, however, a "role" in MoReq2 is something like a user profile - it is not a job or a position, but a set of responsibilities and functional permissions shared by several users. MoReq2 recognises examples of two administrative and two user roles.
203	Administrative roles take actions related to the management of records themselves; their interest is in managing records as entities rather than their content. They also manage the ERMS hardware, software and storage, ensure backups are taken and manage the performance of the ERMS.
3694	Unlike administrative roles, user roles have access to facilities which an office worker or researcher needs when using records. This includes adding documents, searching for and retrieving records; their interest is primarily in the contents of records rather than their management.

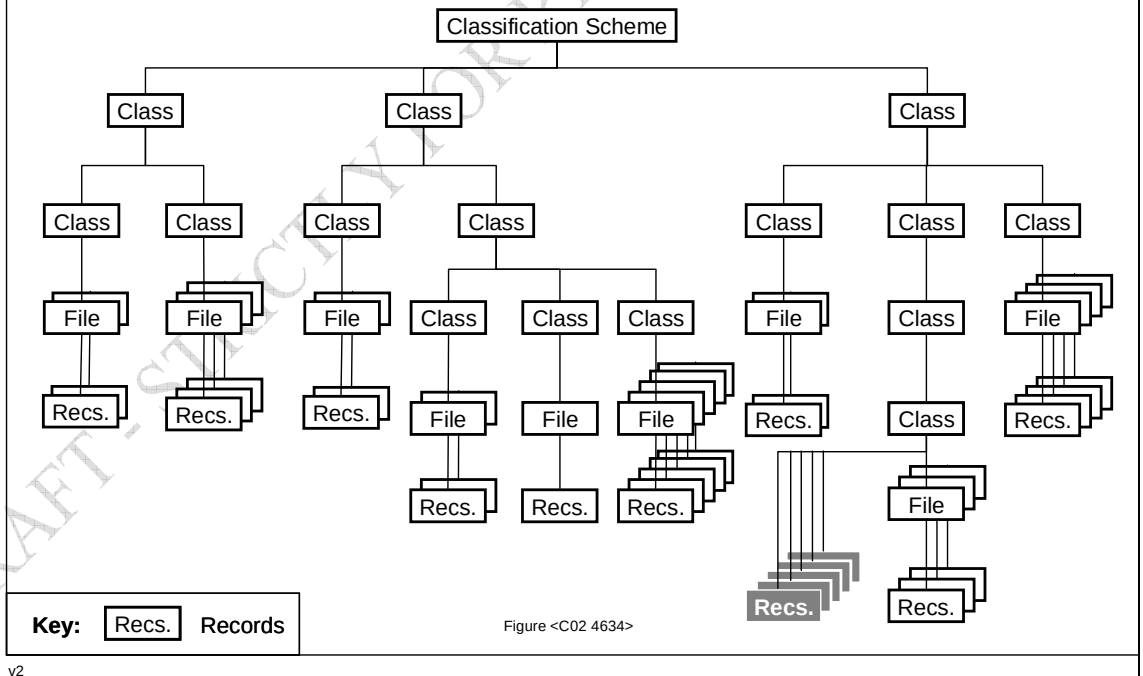
2.3 Entity-Relationship Model

ID	Text
204	**2.3 Entity-Relationship Model**
205	This section contains an entity-relationship model which can be used as an aid to understanding the specification. Section 13.3 contains a narrative explanation.
206	An important aspect of this diagram is that it need not represent actual structures stored in the ERMS. It represents a theoretical view of the entities associated with records. An ERMS uses these relationships to produce behaviour equivalent to the structures in the diagram. See section 2.2 for further explanation of this point.
207	The relationships between files, volumes, records and other important entities are depicted in the following entity-relationship diagram. This is a formal representation of selected structures which can be used to describe the behaviour of an ERMS.

ID	Text
204	**2.3 Entity-Relationship Model**
208	In the diagram, entities - files, records and so on - are represented by rectangles. The lines connecting them represent the relationships between the entities. Each relationship is described by text in the middle of the line; and this should be read in the direction of the arrow. Each end of the relationship has a number which represents the number of occurrences (strictly, the cardinality); the numbers are explained in the key. So, for example, the following extract:
3353	
209	means “one record is made up of one or more components” (note the direction of the relationship arrow).
210	Note that the entity Class is related to itself by the relationship “is made up of”. This recursive relationship describes, in formal terms, the hierarchy of folders, in which a Class may contain other Classes. If this relationship (sometimes called a recursive relationship) is not implemented, the model applies equally to non-hierarchical relationships.

ID	Text
204	**2.3 Entity-Relationship Model**
3354	

3 Classification Scheme

ID	Text, Requirement & Rationale	Testable
211	**3 Classification Scheme and file organisation**	
213	This chapter lists requirements for management of the classification scheme and of the organisation of files. It first lists requirements for setting up the classification scheme in section 3.1. It then lists requirements relating to classes and files (section 3.2) and volumes and sub-files (section 3.3). Section 3.4 lists requirements associated with maintenance of the classification scheme and section 3.5 covers navigation issues.	
212	A classification scheme is the foundation of any ERMS, as described in detail in section 2.2. It allows an electronic record to be stored together with other records that provide its context, by defining the way in which the electronic records will be organised into electronic files, and the relationships between the files.	
4192	A significant difference between MoReq2 and its predecessor is that MoReq2 allows the declaring of a record directly into a class, as well as into a file. The original MoReq did not allow declaration into directly into a class; it allowed only declaration into a file.	
4193	MoReq2 thus allows a record to be captured into any of the following: • Class; • File; • Sub-File; • Volume.	
4633	This is illustrated in the following diagram, which adds such records (shaded in grey) to the illustrations in section 2.1.	
4634	 Figure <C02 4634> v2	
4194	This change has been introduced primarily to reflect the requirements of high-volume case management type systems. For example a large number of records such as licence applications can be allocated directly to a class, without the need to open and manage one or more files.	

ID	Text, Requirement & Rationale	Testable
211	**3 Classification Scheme and file organisation**	
4195	This change is, however, not meant to remove the necessity for a hierarchical classification scheme, or (in most cases) for the existence of files. Rather it is meant for special circumstances (such as high volumes of simple case documentation). Inappropriate use of this feature will introduce the risk of later difficulties in managing records, and users of MoReq2 are advised to use this functionality only after careful analysis. Most users of MoReq2 are unlikely to require this functionality, and so MoReq2 includes the requirement that this functionality can be disabled.	
2779	**Note to reviewers: in a significant change since the previous release, almost all mention of non-hierarchical classification has been removed. This is after lengthy and spirited debate, taking into account strongly-held views on both sides of the argument. This decision, ratified by the MoReq2 Editorial Board, is final.**	
2780	MoReq2 compliance requires support for hierarchical classification. This is because:	
2782	• hierarchical schemes are able to ensure an effective, stable and clear organisation of records; • hierarchical schemes are the most widely used in Europe.	
4653	It also maintains compatibility with the previous version of MoReq. Many requirements use the concept of class. In many cases, it may be possible to apply the requirement to non-hierarchical classification schemes; but this may not always possible.	
4188	It is essential that the classification scheme (technically, a records classification scheme) is closely aligned with the business needs of the organisation. Good practice suggests that the organisation first identifies a business classification scheme before designing a records classification scheme.	

3.1 Configuring the Classification Scheme

ID	Text, Requirement & Rationale	Testable
214	**3.1 Configuring the Classification Scheme**	
2080	**Requirement**	
2089	The ERMS must support and be compatible with the organisation's business classification scheme.	N
2762	*This requirement is not testable in the general case; it is included as a reminder to users of MoReq2 of the need to align the classification scheme used by an ERMS with the business needs of the organisation, as should be reflected by the arrangement of records external to the ERMS.*	
2112	The ERMS must maintain internal integrity (relational integrity or otherwise) at all times, regardless of: • maintenance activities; • other user actions; • failure of system components.	P
2690	*In other words, it must be impossible for a situation to arise where any user action or any software failure results in an inconsistency within the ERMS or its database.*	
3355	The ERMS should allow administrative roles to label each classification scheme with an Identifier, Title, and Description.	Y
3356	*This metadata will support functions such as export of the classification scheme and of records.*	

ID	Text, Requirement & Rationale	Testable
214	**3.1 Configuring the Classification Scheme**	
2088	The ERMS must be able to support a classification scheme which can represent files and records as being organised in a hierarchy of classes.	Y
2763	*The use of a hierarchical classification scheme is mandatory for compliance with MoReq2.*	
2660	*Three levels are a minimum; more levels will be needed in many environments.*	
2715	The ERMS must allow management of the classification scheme by an administrative role only, subject to requirement <ID 2765>.	Y
2764	*In this requirement, "management" refers to the operations described in section 3.1 and section 3.4.*	
2765	The ERMS should allow individual classes to be managed by specified user roles and/or by a specified group of users.	Y
2766	*In the above requirement, "management" has the same meaning as in the preceding requirement. This is intended for two settings:* • *large classification schemes which are too large to be maintained centrally (and which therefore have central management for the higher levels and distributed management for the lower levels);* • *classification schemes that include classes for the management of case files, which need to be managed in the business unit dealing with the cases on allocation of authorised user privileges.*	
2081	The ERMS should not limit the number of levels in the classification scheme hierarchy.	P
2767	*In most settings, it is unlikely that the number of levels needed could be more than ten.*	
2082	The ERMS must allow the titling mechanism(s) to be defined at configuration time by an administrative role**.**	Y
2692	The ERMS should allow the input of textual scope notes (also known as descriptions) to all classes and all files.	Y
3674	*Scope notes are narrative intended to clarify the intended contents and/or exclusions of classes and files for the benefit of users.*	
2087	The ERMS must support the preparation of a classification scheme at configuration time in readiness for the capture and/or importation of electronic records.	Y
2768	*This requirement is intended to allow a classification scheme to be prepared while the ERMS is being configured, and before it is used for the management of records.*	
2677	The ERMS should support the importing of all or parts of a classification scheme, at configuration time or at any other time.	Y
2769	*This requirement is intended to allow a classification scheme to be prepared while the ERMS is being configured implemented, and before it is used for the management of records. Where any part(s) is (are) imported, this may be to add to an existing scheme, or to create a new classification scheme if none exists.*	
2693	Where the ERMS supports the import of all or part of a classification scheme it must allow the import of the associated metadata, retention and disposition schedules and audit trails if these exist.	Y
2770	*In ideal cases, the classification scheme that is being imported will have class metadata and retention and disposition schedules. In other cases, these may be absent or incomplete.*	
2771	Where the ERMS imports the metadata of a classification scheme, it must reject any class that does not have a title, and create an exception report for an administrative role listing the classes that were rejected.	Y

ID	Text, Requirement & Rationale	Testable
214	**3.1 Configuring the Classification Scheme**	
2772	*In an ERMS that is not MoReq2 compliant it may be possible for a class to have no title (a null value); but such a class would be impossible to use within a MoReq2-compliant ERMS.*	
2773	Where the ERMS imports the metadata of a classification scheme, and where the ERMS uses a scheme that features hierarchical numbering (see <ID2099>), the ERMS must assign to each imported class a hierarchical code in one of the following ways, according to an option set by an administrative role: • following the same rules as would be used for the manual creation of the classification scheme; • keeping the original codes in their entirety (only possible if the structures are compatible); • appending the original codes to the codes in the receiving scheme.	Y
2774	*If a hierarchy that is being imported already includes hierarchical class codes (for example 4/6/4) it may not be possible to use these as codes in the ERMS, as consistency and uniqueness cannot be guaranteed.*	
3753	*There are many possible scenarios for such an import, with different kinds of incompatibility between hierarchical numbering schemes. MoReq2 does not prescribe the outcome of an attempt to select an option that is logically impossible because the schemes are incompatible.*	
3754	*If the existing codes cannot be used, they can be treated as appropriate to the situation, e.g. copied to a metadata element called "old class code".*	
2775	Where the ERMS imports the metadata and disposition authorities of a classification scheme, it must validate them using the same rules as would be used for the manual creation of the classification scheme (see chapter 12). Where this validation process finds errors (for example the absence of mandatory metadata, or format errors) it must bring these to the attention of the administrative role performing the importation, identifying the metadata involved.	Y
2776	*In ideal cases, the classification scheme that is being imported will have metadata (e.g. metadata for its classes) that complies fully with the MoReq2 metadata model. In other cases, the metadata may be non-compliant. In these cases, several outcomes are possible; MoReq2 does not mandate any one outcome. Possible outcomes include:* • *The entire importation is cancelled and the administrative is informed of the reason for the cancellation;* • *Importation of the class that has non-compliant metadata is cancelled and the administrative role is informed of the reason for the cancellation;* • *The administrative role is required to choose between correcting the error and cancelling importation of the affected class;* • *Importation continues even though part of the metadata is non-compliant, with non-compliant data being replaced by default values specified for the affected elements and an error report produced.*	
3755	*Informing the administrative role does not require that the process be a foreground, or real-time process; it will be acceptable for the process to be a background, or batch, process.*	
2696	The ERMS should support the export of all or part of a classification scheme.	Y
2697	Where the ERMS supports the export of all or part of a classification scheme this must include associated metadata, an administrative role being able to select which metadata is exported.	Y

ID	Text, Requirement & Rationale	Testable
214	**3.1 Configuring the Classification Scheme**	
2699	Where the ERMS supports the export of all or part of a classification scheme this must include all associated disposition authorities at the option of an administrative role.	Y
2777	Where the ERMS supports the export of all or part of a classification scheme, this must include all or selected audit trail data, the selection to be made by an administrative role.	Y
3175	Where the ERMS supports export (for any of the above requirements) it must use a fully-documented format.	
3176	Where the ERMS supports export (for any of the above requirements) it should export the information in XML or equivalent open standardised format.	
2718	Where the ERMS supports the copying of all or part of a classification scheme this must include all associated metadata.	Y
2720	Where the ERMS supports the copying of all or part of a classification scheme this must include all associated disposition authorities.	Y
2086	The ERMS must allow administrative roles to add new classes at any point within any class, so long as files are not stored at that point.	Y
3628	*MoReq2 does not allow files and classes to exist at the same level within a class (in other words, files and classes cannot be mixed at a single node in the classification scheme hierarchy). This is for reasons of good records management practice.*	
2084	The ERMS should support the definition and simultaneous use of multiple classification schemes.	Y
2662	*Most organisations will mandate that a single classification scheme be used for the primary classification of all the files in the ERMS. This requirement allows some of the files in the ERMS to belong to one classification scheme while other files belong to another. This may be required, for example, following the merger of two organisations, or when different collections of records in a single organisation require different management regimes.*	

3.2 Classes and Files

ID	Text, Requirement & Rationale	Testable
236	**3.2 Classes and Files**	
237	This section lists requirements which apply to classes and files. Classes and files are different kinds of construct. Classes provide an intellectual framework for classification, while files aggregate records; classes are building blocks of classification schemes, while files are not. Despite these major differences, it is helpful to list some requirements together, as they are common to both constructs.	
2090	**Requirement**	
4218	The ERMS must allow an administrative role to configure whether a class so that it can, or so that it cannot, store records directly.	
4219	*In other words the system must be able to be configured so that records do not have to be held in files, sub-files or records.*	
2100	The ERMS must support the capture, maintenance and presentation of metadata for files and classes in the classification scheme, compliant with the MoReq2 metadata model.	Y
2664	The ERMS must restrict the ability to add to file and class metadata as set out in the MoReq2 metadata model.	N
2099	The ERMS must provide a mechanism for allocating automatically a hierarchical classification code (where such a code does not already exist - see <ID 2773>) to each class, file, sub-file and volume in the classification scheme.	Y

ID	Text, Requirement & Rationale	Testable
236	**3.2 Classes and Files**	
2665	The ERMS must allow user roles to allocate a title for each electronic class, file, sub-file and volume.	Y
2786	*This requirement applies to non-case file environments. Where case file management is needed, an alternative naming approach is needed. This is specified in chapter 10.6.*	
2666	It must be possible to use both the classification code and textual file title separately or together.	Y
2700	The ERMS must allow an administrative role to configure the classification code.	Y
3740	*Configuration of the classification code should include:* • *the format of the identifier associated with each level of the hierarchy, e.g. numeric, alphabetic;* • *the first value of this identifier at each class, e.g. 1, 1000;* • *the interval to be used between successive classes, e.g. 1, 10;* • *the presence or absence of leading zeroes;* • *any global prefix, e.g. "corporate/";* • *any global extension, e.g. country suffix;* • *the separator between each identifier, e.g. "/", "-".*	
2789	The ERMS must record the date of opening and the date of closing of a class or file within the class or file's metadata.	Y
2790	*The date of opening and closing of a class or file provide important context for the records classified within it.*	
3632	*When a class or file is open, it is possible to capture records into it. When a class or file is closed, it is not possible to capture records into it.*	
2701	The ERMS must record the date of creation of a new class or file in the metadata of the class or file.	Y
2791	*In the case of physical files, it is possible for the date of opening to be earlier than the date of creation recorded in the ERMS. This can arise if a physical file is created and opened, in physical form only, before it is created in the ERMS.* *In the case of electronic files, it is possible for the date of opening to be earlier than the date of creation recorded in the ERMS. This can arise when an electronic file is imported into the ERMS from another system.*	
2096	Whenever a new class or file is opened, the ERMS must automatically include in its metadata those attributes which are inherited due to its position in the classification scheme.	Y
2676	*For example, if a "Correspondence" file is in a hierarchical path titled:* *Regional plan development : Public consultation : Correspondence* *and an administrative role adds a new file titled "Formal Objections" at the same level as the "Correspondence" file then the new file must automatically inherit the prefix Regional plan development : Public consultation.*	
2667	The ERMS must allow an administrative role to modify inherited metadata values, to the extent permitted by the MoReq2 metadata model.	Y
2680	*Inherited values often provide a default, or starting position. This can be changed, so long as the change is compatible with the metadata model.*	
2668	Any addition to this inherited metadata should be inherited by default by all descendant classes and files.	Y
2093	The ERMS should support the allocation of controlled vocabulary terms compliant to ISO 2788 as descriptive class or file metadata subject terms, in addition to the other requirements in this section.	Y

ID	Text, Requirement & Rationale	Testable
236	**3.2 Classes and Files**	
3635	The ERMS should support the allocation of controlled vocabulary terms compliant to ISO 5964 as descriptive class or file metadata subject terms, in addition to the other requirements in this section.	Y
3636	*Requirements <ID2093> and <ID3636> are identical save that the former specifies a monolingual thesaurus and the latter a multilingual thesaurus.*	
2092	The ERMS must not impose any practical limit on the number of classes or files which can be defined.	P
2091	The ERMS must be able to print a list (sometimes referred to as a repertory) of all files or of files classified against a specific class (and its descendant classes).	Y
3639	A user printing a list of files (as in <ID2091>) should be able to specify the sequence, content and format of the list.	Y
3640	*For example, the user should be able to sort in ascending or descending order, on title or code, and preferably on any attribute; and should be able to specify the metadata attributes to be printed.*	
2681	The ERMS should be able to export a list, or repertory, of all files or of files classified against a specific class (and its descendant classes) in XML format and/or in a human-readable format.	Y
2682	The ERMS must allow the classification scheme to be printed, both as a complete scheme and as any class selected from the scheme.	Y
3641	A user printing a classification scheme (as in <ID2682>) should be able to specify the content and format of the scheme.	Y
3642	*For example, the user should be able to should be able to specify the metadata attributes to be printed, and preferably choose a list, or indented, or graphical representation.*	

3.3 Volumes and Sub-Files

ID	Text, Requirement & Rationale	Testable
261	**3.3 Volumes and Sub-Files**	
2797	In a system that keeps paper records, subdivision of large files is essential for reasons of ergonomics and the physical survival of folders, binders, jackets etc. Typically, for example, paper files are limited to 2cm in thickness, by the establishment of volumes. When the file reaches the size limit (2cm thick in this example), it is considered to be a closed volume and a new volume is opened. This is not true of electronic files - an electronic file can usually grow to almost any size without such difficulties.	
2798	However, in practice, there can be benefits in splitting large electronic files into volumes. These benefits are, for example: • when users need to work remotely (that is, over low-bandwidth connections, or after downloading records to a portable PC, or onto a storage device with limited capacity); • when files are never closed, because they are (for example) geographically linked.	
3645	Similarly, paper files are often divided into sub-files - especially in case management environments. The sub-files are used to organise the file contents, often according to document type.	

ID	Text, Requirement & Rationale	Testable
261	**3.3 Volumes and Sub-Files**	
3646	Correspondingly, there are sometimes benefits in dividing electronic files into sub-files, for example: • improving the ease of navigation through a file; • providing a means to manage document types that have specific needs, such as documents that cannot be scanned cost-effectively.	
262	This section includes requirements relating to the use of volumes and sub-files, both of which are typically used to subdivide files which might otherwise be unmanageably large. However, Moreq2 does not mandate that these subdivisions be implemented; it merely requires that MoReq2 compliant software must be able to provide them when needed.	
2793	*Sub-files were not recognised in the previous version of MoReq.*	
2794	In summary: • Each file contains one or many sub-files; • Each sub-file contains one or many volumes; • Volumes of different sub-files are created independently; • All the sub-files of an open file are always open, and all the sub-files of a closed file are always closed; • Only one volume can be open in each sub-file. For more detail about sub-files and volumes, see section <insert reference here>.	
3651	**Requirements**	
4201	It must be possible for an administrative role to configure the ERMS to remove the ability to create sub-files and/or volumes within files across the classification scheme.	Y
4199	It must be possible for an administrative role to configure the ERMS to allow only sub-files to be created within files within an area of the classification scheme.	Y
4200	It must be possible for an administrative role to configure the ERMS to allow only volumes to be created within files within an area of the classification scheme.	Y
3652	When a file contains only one sub-file, it is acceptable for the file and sub-file to be indistinguishable to end users.	N
3653	When a sub-file contains only one volume, it is acceptable for the file and sub-file to be indistinguishable to end users.	N
3654	When a file contains only one sub-file which itself contains only one volume, it is acceptable for all three to be indistinguishable to end users.	N
3655	*The intention of the three requirements above is to emphasise that the ERMS must not impose on users the structure of "file, sub-file, volume". The ERMS should allow the use of sub-files and volumes, while allowing users to think in terms of files only if this suits them.*	
4198	*The essence of this is that the user only sees what is essential from a business process point of view and in not encumbered by potentially confusing choices.*	
2104	The ERMS must support the concept of open and closed electronic volumes, as follows: • only the most recently created volume within a sub-file can be open; • all other volumes within that file must be closed.	Y
2107	The ERMS must allow administrative roles to add an electronic volume to any electronic sub-file which is not closed.	Y
2795	*The process of adding a new volume consists of closing the volume that is currently open and creating a new open volume.*	
3650	The ERMS must allow administrative roles to add sub-files to any electronic file which is not closed.	Y
2106	The ERMS must record the date of opening of a new volume or sub-file in the metadata.	Y

ID	Text, Requirement & Rationale	Testable
261	**3.3 Volumes and Sub-Files**	
2105	Whenever a new volume or sub-file is opened, the ERMS must automatically include in its metadata those attributes of its parent file's metadata which are common (as defined in the MoReq2 metadata model).	Y
2685	*Records in a volume can be accessed regardless of whether the volume is open or closed.*	
3671	Whenever a new volume is opened, the ERMS must automatically assign to it an identifier that is unique within its parent sub-file.	P
3672	*The identifier could be a simple sequence number, starting at 1 for each sub-file.*	
2758	When classifying a record the user must be presented with the most recently created volume in the chosen sub-file by default.	Y
2670	The ERMS must allow the creation of multiple concurrent open sub-files within any file.	Y
2115	The ERMS must record the date of closing of a volumes and files in their metadata.	Y
2103	The ERMS must prevent the user from adding electronic records to a closed volume.	Y
2102	The ERMS must allow an administrative role (not user roles) to add a record to a previously-closed volume; and must require that an administrative role adds a comment to the metadata of both the volume and the record, and to the audit trail, explaining why this exception has taken place. This action must not update the date of closure stored in the metadata.	Y
4206	*This applies only if the newly added record is not younger than the date of closure of the volume.*	
2671	*This facility is intended to be used to rectify user error, e.g. if a volume was closed unintentionally. For this reason, it is important that the exception causing this action is properly documented.*	
3658	*MoReq2 does not mandate how this is achieved. It may be achieved by temporarily re-opening the closed volume, or by other means.*	
3659	The ERMS must allow an administrative role to delete an empty volume.	Y
3660	The ERMS must allow an administrative role to delete an empty volume and re-open the previous volume in the sub-file, in a single action, recording the event in the audit trail.	Y
3661	*This is intended to correct an error which has resulted in the incorrect closure of a volume.*	
2799	The ERMS should allow a "template" of sub-files to be created for a specified class, such that the template specifies the sub-files to be created automatically for each new file that is subsequently created in that class.	Y
2800	*This is intended primarily for case management environments. As an example, a template in an insurance company might specify, for the class dealing with client insurance policies, the following sub-files: policy and amendments, internal correspondence, correspondence with medical specialists, billing, other client correspondence. Thereafter, every new file created in that class would automatically be created with these sub-files.*	
2801	The ERMS must automatically close all sub-files in a file when that file is closed.	Y
3656	The ERMS must allow users to close volumes individually.	Y

3.4 Maintaining the Classification Scheme

ID	Text, Requirement & Rationale	Testable
2658	**3.4 Maintaining the Classification Scheme**	
2659	**Requirement**	

ID	Text, Requirement & Rationale	Testable
2658	**3.4 Maintaining the Classification Scheme**	
2123	The ERMS must allow an administrative role (not a user role) to relocate a class or file to a different position in the classification scheme. As part of this relocation the ERMS must ensure that all electronic records already allocated remain allocated to the class (es) file(s) and volume(s) and sub-file(s) being relocated.	Y
2673	*This facility is intended for exceptional circumstances only, such as organisational mergers or other re-organisation, or to correct clerical errors. This requirement must be read together with <insert reference>.*	
2717	The ERMS should support the copying any class (and its descendant classes) of a classification scheme to another point in the classification scheme.	Y
3179	*This facility is intended for use when replicating branches of a classification scheme, an act that is sometimes required (for example) when designing a part of the scheme is not strictly functional.* *Use of export followed by import will not be considered sufficiently easy to meet this requirement.* *Any conflicts of code should be handled in the same way as with an import (see <insert reference>).*	
2122	The ERMS must allow an administrative role (not a user role), to reclassify an electronic record to a different class, volume or sub-file.	Y
2688	*This facility is intended for exceptional circumstances only, such as to correct user errors. This requirement must be read together with <ID2121>, <ID2120> and <ID2119>.*	
2674	Upon reclassification or relocation of a class, file, sub-file, volume or record the ERMS must enable the optional inheritance of defined metadata according to its new position in the hierarchy.	Y
2120	When any classes, files, or records are relocated or reclassified the ERMS must keep a clear trace of their status prior to the relocation or reclassification in the audit trail.	Y
3664	When any classes, files, or records are relocated or reclassified the ERMS must record the values of their metadata prior to the reclassification.	
2675	*Both of the above requirements are in support of the need to be able to determine the history of classes, files etc. that have been relocated or reclassified.*	
2119	When any classes, files, volumes, sub-files or records are relocated or reclassified the ERMS must require an administrative role to enter as metadata the reason for the reclassification.	Y
3665	*Entry of a reason is mandatory, as these relocations and reclassifications are exceptional, potentially endangering the integrity of the records if not carefully managed.*	
2707	The ERMS should enable an administrative role to mark a class as inactive to prevent any new files being added to that class.	Y
2708	The ERMS should allow an administrative role to delete an empty class.	Y
2118	The ERMS must prevent the deletion of an electronic file or any part of its contents at all times, with the exceptions of: destruction in accordance with a retention and disposition schedule - see chapter 5; or deletion by an administrative role as part of an audited procedure - see section 9.3.	Y
2117	The ERMS must allow an electronic file to be closed by user roles.	Y
3666	*This is different than the corresponding requirement in MoReq, which limited this function to administrators.*	

ID	Text, Requirement & Rationale	Testable
2658	**3.4 Maintaining the Classification Scheme**	
2116	The ERMS should be able to close an electronic file volume automatically on fulfilment of specified criteria to be defined at configuration, including at least: • volumes delineated by an annual cut-off date; for example, the end of the calendar year, financial year or other defined annual cycle; • the passage of time since a specified event; for example, the most recent addition of an electronic record to the volume; • the number of electronic records which the volume contains.	Y
2689	*Other criteria may be desirable in particular circumstances, for example when the size of the volume reaches the storage capacity of a removable disc.*	
2704	The ERMS must make the contents of closed classes, files, sub-files and volumes as accessible for viewing as those that are open, without making any differentiation between open and closed.	Y
3667	*In other words, users who are searching for browsing through information using the ERMS must not have to be aware of whether files etc. are closed or open; and the same search facilities and access rules must apply.*	
2113	The ERMS should allow users to create cross-references (that is, "see also" type links) between related files.	Y
2111	The ERMS should support the ability to create multiple entries for an electronic record, in several electronic classes, files, sub-files or volumes, without duplication of the record or of the document on which it is based.	Y
2691	*MoReq2 does not specify how this is achieved. One way of supporting this requirement would be to use pointers when capturing more than one record based on the same document.*	
2110	The ERMS must provide reporting tools for the provision of statistics to administrative roles on aspects of activity within the classification scheme, including the numbers and sizes of classes, files, volumes, sub-files or records created, closed or deleted within a given period. Reporting should be both overall and by any specified user or class.	Y
3670	The ERMS should provide ad hoc reporting capabilities on aspects of activity within the classification scheme.	P
2053	Any user working with a class, file or record must be able to discover easily and quickly the context of that class, file or record, or in other words, the metadata and parent file or class(es); and must be able to navigate to these parents from the class, file or record.	Y
2802	*It must be possible to discover the context without having to leave the class or file, in a way that allows work with the file to be continued without interruption.*	

4 Controls and Security

ID	Text, Requirement & Rationale	Testable
310	**4 Controls and Security**	
311	This chapter brings together requirements for a wide range of controls which relate to the security of the records. These requirements provide features needed to protect the characteristics of records defined in ISO 15489 (section 7.2).	
312	It is essential that organisations are able to control who is permitted to access records and in what circumstances, as records may contain personal, commercial or operationally sensitive data.	

ID	Text, Requirement & Rationale	Testable
310	**4 Controls and Security**	
3182	Restrictions on access may also need to be applied to external users. For example, in some countries where freedom of information legislation permits access to selected public records, customers may wish to view records. Also some organisations may wish to share parts of their ERMS repository with partner organisations. Requirements for these controls are listed in section 4.1.	
313	Any access to records and all other activities involving them and related documents or data also need to be recorded in the audit trail to ensure legal admissibility and to assist in data recovery. Requirements for these audit trail controls are listed in section 4.2; these requirements address principally the record characteristics of authenticity and integrity defined in ISO 15489 (section 7.2).	
314	Security of records also includes the ability to protect them from system failure by means of backup, and the ability to recover the records from backups. These requirements are listed in section 4.3; these requirements are related to the record characteristic of usability defined in ISO 15489 (section 7.2).	
3183	Vital records are mission-critical records that need to be recovered rapidly after a disaster. These are addressed in section 4.4.	

4.1 Access

ID	Text, Requirement & Rationale	Testable
318	**4.1 Access**	
319	Organisations need to be able to control access to their records and typically this is achieved by the specification and implementation of security policies, i.e. access to records is granted based on the business role an individual plays in the organisation. Users are usually managed centrally and simultaneously granted access rights to a number of corporate systems, including but not restricted to the ERMS.	
3184	It is not considered best practice to manage permissions in an ERMS simply by allocating individual permissions on individual entities to individual users. Access rights will therefore normally be granted to roles and/or groups to allow them to save and refer to records in specified classes or files within the classification scheme.	
4455	In addition to the entitlement to access specific parts of the classification scheme, permissions also restrict the actions that a user, role or group can perform on entities within the ERMS, such as inspecting their metadata or their contents, modifying or deleting them and creating or viewing entities of a particular type.	
4456	For example, a user role can search for and read records, but role-based security organisation may restrict the capability to search and read to particular sub-sets of the ERMS.	
4457	Permissions can be applied to groups and be inherited by the group members. Applying permissions at the group level, rather than the user level improves the management of the ERMS over time as new users arrive, and existing users change and leave.	
4458	Through the creation of roles in the ERMS multiple permissions can be granted to a user or group automatically. Later, when the user or group is removed from the role all the permissions are automatically rescinded.	
320	The ERMS must be able to limit the setting of these access rights to certain roles. In the table in 13.4, this is shown as belonging to administrative roles.	

ID	Text, Requirement & Rationale	Testable
318	**4.1 Access**	
3185	Note, however, that administrative roles are only implementing, from a system perspective, policy decisions taken by more senior management. The security polices and their allocation to individual end users, are typically based on the business needs of users to access information, the organisation's records policy and laws and regulations, such as information laws, data security laws, archival laws and industry regulations; these are addressed in section 11.5.	
4459	In some environments, ERMS access permissions are managed entirely within the ERMS. In others, some permissions are managed using separate software, such as a network operating system utility. Either is acceptable for compliance with the following requirements.	
4460	The roles identified are "indicative" only. It should be the organisation that sets the number and the make-up of the roles that it uses and even whether it uses roles at all, according to its own requirements.	
2124	**Requirement**	
4391	The ERMS must not allow any person to carry out any action in the ERMS unless the person is an authorised user who is successfully identified and authenticated.	Y
4392	*MoReq2 does not specify the nature of the authentication mechanism. In many situations, a user-id and password mechanism is considered to provide sufficient authentication. Organisations using MoReq2 for procurement purposes need to ensure that an appropriate level of authentication is included.*	
2136	The ERMS must allow administrative roles to allocate access to records, sub-files, files classes and metadata to specified user roles or user groups and for specified periods of time.	Y
4214	The ERMS must not place a limit on the number of roles that can be configured.	P
2135	The ERMS must allow administrative roles to maintain permissions for all roles. These determine the functionality, metadata elements, records or files to which the roles have access, and the kinds of access allowed.	Y
3186	The permissions will: • prohibit access to the ERMS without identification and authentication; • allocate access according to the organisation's security policies; • restrict access to specific aggregations, files or records; • restrict access to specific classes of the classification scheme; • restrict access according to the user's security clearance; • restrict access to particular features and functions (e.g. read, up-date and/or delete specific metadata elements); • deny access after a specified date.	Y
3187	*An example of an accepted authentication mechanism is a logon id and associated password.*	
3226	The ERMS should allow configuration to enable access by means of an integrated network log-on.	Y
3202	The ERMS must allow administrative roles to add and remove users to and from groups at any time.	Y
4448	*It is acceptable for administrative roles to manage groups by means of separate directory management software.*	
3229	The ERMS must allow the allocation of administration rights over different sections of the classification scheme to different administrative roles.	Y
3230	*For example see the access control model in chapter 13.4.*	

ID	Text, Requirement & Rationale	Testable
318	**4.1 Access**	
3227	The ERMS must allow administrative roles to mark an individual user as inactive, without deleting the user from the system.	Y
4164	*It is acceptable for administrative roles to manage users by means of separate directory management software.*	
2134	The ERMS must allow administrative roles to define the same control functions for user roles as for users.	Y
3203	*This feature allows administrative roles to manage and maintain a limited set of role access rights rather than a larger number of individual users. Examples of roles might include Manager, Claims Processing Clerk, Security Analyst, Database Administrator.*	
3239	The ERMS must be able to apply selections of access requirements across roles.	Y
4450	*For examples see chapter 13.4.*	
2133	The ERMS must allow an administrative role to set up and maintain groups of users.	Y
3188	*Examples of groups might be Human Resources, Northern sales team.*	
2132	The ERMS must allow a user to be a member of more than one group.	Y
3201	*It is likely that some users will have different access requirements for different parts of the classification scheme.*	
3205	The ERMS must allow administrative roles to set up ad hoc lists of individual users in order to control access to specified parts of the classification scheme or records.	Y
2166	The ERMS must restrict systems functions and related events to administrative roles only.	Y
3197	*This is needed to protect the authoritativeness of electronic records.*	
2131	The ERMS must allow only administrative roles to set up user profiles and allocate users to groups and roles.	Y
3204	*See also section 13.4.*	
2130	The ERMS must allow roles with ownership of records to specify which other users or groups can access those records.	Y
3206	*If the organisational policy allows, ownership should be with administrative roles.*	
2129	The ERMS must restrict the ability to make changes, such as adding, amending and deleting profiles for groups, roles or users to administrative roles.	Y
3207	*This includes attributes such as access rights, privileges, password allocation and management.*	
2128	If a user requests access to, or searches for, any object such as a record, volume, sub-file, file or class which the user does not have the permission to access, the ERMS must provide one of the following responses (the response to be selected at configuration time): • display title and other metadata of the object; • display title, type of entity (class, record etc.), date of creation and owner only; • confirm the existence and (optionally) the owner of the object (display its file or record identifier) but not its title or other metadata; • provide no information about the object, thus providing no indication of whether the object does or does not exist; all the above being subject to <ch4 ID 2127>.	Y
3189	*These options are presented in order of increasing security and should be configured by administrative roles. The requirement in the third option (i.e. the most stringent) implies that the ERMS must not include such records in any count of search results; this level of security is normally appropriate for records dealing with matters such as national security or confidential medical records.*	

ID	Text, Requirement & Rationale	Testable
318	**4.1 Access**	
4393	The ERMS should allow the responses specified in <ID2128> to be selected at the object level as an alternative to a system-wide configuration time setting.	Y
2127	If a user performs a content search (typically, but not necessarily, a full text search or free text search, see <section 6.7 ID4490>), the ERMS must not include in the result list any record which the user does not have the permissions to view the content.	Y
3190	*If the first option of <ch4 ID 2128> is chosen, this could be seen to conflict. This apparent conflict is intentional, for if this requirement is not present users may be able to use text searches to investigate the contents of documents to which they are not allowed access. Consequently this requirement must take precedence over requirement <ch4 ID 2128>.*	
3268	The ERMS must allow administrative roles to set up and manage rules to govern users' access to ERMS functions, so that different roles have access to different combinations of functions. The ERMS must allow such rules to be set up with at least the level of granularity (i.e. the amount of breakdown) shown in the illustrative access rights table in section 13.4.	Y
3269	*Different organisations have different functional access control requirements. It is therefore not appropriate to attempt to define a generic model. Accordingly, this requirement specifies instead the level of detail of control that an ERMS must offer.*	
3272	The ERMS must allow administrative roles to create additional roles to those shown in 13.4.	Y
3273	*An organisation could define roles with specific access rights such as: case worker, manager etc.*	

4.2 Audit trails

ID	Text, Requirement & Rationale	Testable
348	**4.2 Audit trails**	
349	An audit trail is a record of actions taken which involve the ERMS. This includes actions taken by users or administrative roles, or actions initiated automatically by the ERMS as a result of system parameters. See the Glossary at section 13.1 for a formal definition.	
3208	The audit trail for records can be viewed as a form of metadata of the individual records (because it consists of information describing some aspects of the records' history), though this is not essential; MoReq2 does not use this view.	
350	The ERMS must be capable of management and control of electronic and physical records according to legislative and regulatory requirements. It must also be capable of demonstrating this compliance.	
4209	The audit trail demonstrates that business rules are being followed and ensures that unauthorised activity can be identified and traced.	
4205	In order to support accountability it is essential that the ERMS is able to record in the audit trail any action where any degree of automated or machine assisted processing is implemented within the system. Chapter 10.6 Casework provides examples of such an interface.	
3209	The audit trail is a key factor in enabling the ERMS to fulfil these requirements by maintaining a complete record of all the actions on every record (within the constraints of the level of assurance of the technical environment).	

ID	Text, Requirement & Rationale	Testable
348	**4.2 Audit trails**	
351	The volume of audit trail information can become large if all actions are audited. Consequently, in some implementations, management may decide that selected actions need not be included in the audit trail (after the date of the decision).	
3210	In many implementations, the on-line audit trail is periodically moved to off-line storage, the off-line copy being subject to deletion if and when the relevant records are disposed of, or if and when policies and legislation permit.	
3199	These are matters of management policy and/or legal/regulatory requirements. This specification therefore includes system requirements to allow these actions, but does not establish the extent to which they are used.	
2137	**Requirement**	
2149	The ERMS must keep an unalterable audit trail capable of automatically capturing and storing information about: • any action taken on any record, any aggregate or the classification scheme; • the user undertaking the action; • the date and time of the action.	Y
2144	*By way of illustration, the actions recorded in the audit trail must include, but need not be limited to:* • *capture of all electronic records;* • *re-classification of an electronic file within the classification scheme (see <ID 2122>);* • *any change to any Retention and Disposition Schedule;* • *any disposition review actions carried out by administrative roles;* • *the placing or removal of a disposal hold on an electronic file;* • *any change made to any metadata associated with classes, electronic files or electronic records;* • *amendment and deletion of metadata by a user;* • *changes made to the access permissions;* • *creation, amendment or deletion of a user or group;* • *export or transfer;* • *creation of a presentation;* • *deletion / destruction of records.*	
4366	The ERMS should be able to record automatically in the audit trail any access to any record or aggregation, whether the access was to read, print or otherwise present it.	Y
4367	*This is normally only required in highly secure environments.*	
3211	The ERMS must not allow the audit trail to be modified by any user, including administrative roles.	Y
3192	*The audit trail may, however, be subject to re-organisation and copying to off-line storage if required by, for example, database software, so long as its integrity remains intact.*	
3237	The ERMS audit trail parameters must be configurable so that administrative roles can configure which actions are automatically recorded.	Y
4210	All changes to audit trail parameters must themselves be audited in the audit trail.	Y
4211	*It should never be possible to turn off the auditing of changes to audit trail parameters so that the ERMS does not record in the audit trail who changed them and when.*	
2148	Once the audit trail parameters have been set, the ERMS must track actions automatically and must store information about them within the audit trail.	Y

ID	Text, Requirement & Rationale	Testable
348	**4.2 Audit trails**	
2147	The ERMS must maintain the audit trail for as long as required by the organisation's records policy.	N
4368	*This often will be at least for the life of the records to which the audit trail refers. However, there may be situations in which other policies apply, for example periodic scrutiny of the audit trail followed by its destruction and replacement by a certificate of scrutiny.*	
2146	The ERMS must log in an audit trail all actions performed on records, volumes, sub-files, files, classes, disposition authorities, and metadata associated with any of these, regardless of whether the action affects one or more of them.	Y
3223	Any annotation of or amendment to a record must be recorded within the record's audit trail.	Y
2145	The ERMS must automatically log in an audit trail all changes made to administrative parameters.	Y
3193	*For example, if an administrative role changes a user's access permissions or reconfigures the audit trail.*	
2806	The ERMS must record in its audit trail the addition of any keyword to any file.	Y
2142	The ERMS must ensure that audit trail data is available for inspection on request, so that a specific event can be identified and all related data made accessible.	Y
3212	The ERMS must include features that allow only authorised users, who have little or no familiarity with the system, to search for information in the audit trail.	P
3270	*This is an ease of use requirement. The users may be external to the organisation, such as external auditors. Nonetheless, from the ERMS perspective they will be users.*	
4363	The ERMS must allow users to search audit trails for specified events, objects (classes, records etc.), users, groups, roles, times, or time intervals.	Y
2141	The ERMS must be able to export audit trail data for specified records, volumes, sub-files, files and classes without affecting the audit trail stored by the ERMS.	Y
3194	*This functionality is to enable, for example, external auditors to examine or analyse system activity.*	
2140	The ERMS must be able to capture and store, where applicable, any attempted violations of access control mechanisms (i.e. a user's attempts to access a record, volume, sub-file or file to which he is denied access).	Y
3195	*For an illustration of circumstances which can allow attempts at violation, see* <ID 2128>. *This cannot apply when the system is configured to hide from a user all knowledge of information to which the user does not have access permissions.*	
4364	Where the ERMS supports the transfer of audit trail data to off-line storage, the ERMS must support secure processes for managing the off-line data and demonstrate how off-line data can be brought back on-line as and when required; and the ERMS must ensure it is not possible for this mechanism to be used as a means of by-passing the controls imposed by the ERMS (i.e. by simply moving audit trail data out of the ERMS and changing or deleting it externally to the system).	P

4.3 Backup and Recovery

ID	Text, Requirement & Rationale	Testable
379	**4.3 Backup and Recovery**	

ID	Text, Requirement & Rationale	Testable
379	**4.3 Backup and Recovery**	
380	Business and regulatory demands require that an ERMS be provided with comprehensive controls to provide regular backup of the records and metadata; and to be able rapidly to recover records if any are lost because of system failure, accident, security breach etc.	
381	Regular automated backup and recovery can be provided by the ERMS, or by integration with the services or utilities of an Electronic Document Management System (EDMS), by a database management system operating with the ERMS, or by some other software component application. In this section, references to "the ERMS" can mean any of these, as appropriate to the setting.	
382	In practice, backup and recovery functions may lie more with the organisation's IT operations area than divided between ERMS administrative roles.	
2150	**Requirement**	
2157	The ERMS must provide or allow automated backup and recovery procedures that allow for regular backup of all or selected classes, files, records, metadata, administrative parameters, and the audit trail of the ERMS; and their recovery when needed.	Y
2156	The ERMS must allow administrative roles to schedule backup routines by: • specifying the frequency of backup; • selecting classes, files or records to be backed up; • allocating storage media, system or location for the backup (e.g. off line storage, separate system, remote site).	Y
2155	The ERMS must allow only authorised roles to restore from ERMS backups.	Y
4370	When an ERMS restores from a backup, full integrity of the data including the audit trail must be maintained after the restore.	P
2154	Where the ERMS features checkpoints and database roll-forward facilities, the ERMS must allow only authorised administrative roles to roll it forward.	P

4.4 Vital Records

ID	Text, Requirement & Rationale	Testable
2054	**4.4 Vital Records**	
2055	Vital records are the records that are considered absolutely essential to the organisation's ability to carry out its business functions, in the short term, in the long term or both. This can be either mission-critical in terms of its ability to cope with emergency/ disaster conditions or to protect its long-term financial and legal interests.	
3214	The identification and protection of such records is of great importance to any organisation and it is likely that it is these records that will need to be recovered first in the event of a disaster.	
3217	Records may be considered as vital records either for the organisation as a whole or part of the organisation.	
3271	**Requirement**	
2152	The ERMS must allow administrative roles to indicate that selected files or records contain, or are considered to be, "vital records".	Y
3196	*This indication should be included as a metadata element.*	
2151	The ERMS must provide two separate back-up operations: • "full" backup, which backs up all (specified) ERMS data; • "vital" backup, which backs up only the ERMS configuration and files identified as "vital".	Y

ID	Text, Requirement & Rationale	Testable
2054	**4.4 Vital Records**	
4371	*Two back-up operations are used for the following reasons to allow:* • *"vital" back-ups to be scheduled more often than "full" ERMS back-ups;* • *"vital" back-ups to be taken onto different media and stored separately from (and possibly more securely than) "full" back-ups.*	
4372	*It also provides for better managed ERMS restoration where restoring from "vital" back-ups can occur entirely independently of and at a different time to "full" restoration.*	
4373	The ERMS must provide for system recovery back to full operation after recovering from a "vital" back-up.	Y
4374	*After restoring from a "vital" back-up many files and records will not be present. Other than this, however, the ERMS should not be in any way limited in its operation or the functionality that it provides to users*	
4375	The ERMS should provide for two methods of restoring from a "full" back-up: • restoration to a "clean" environment, in which the data from the "full" back-up overwrites and replaces the ERMS during the recovery operation; • restoration over an existing environment, in which the data from the "full" back-up is merged back into an existing ERMS environment.	Y
4376	*The first method of restoration will be common in organisations where "vital" back-ups are not taken. The second method of restoration will occur when an ERMS has previously been partially restored from a "vital" back-up and returned to normal operation; it then becomes necessary to merge in the "full" back-up without overwriting either the vital files that were previously restored or any new entities that have been added, or changes that have been made, to the ERMS in the interval since it was returned to full operation.*	
4377	*The "vital" back-up (if it exists) will always be restored first. There is no need to consider the restoration of a "vital" back-up over a "full" back-up.*	
4378	*When undertaking a two-part system restoration in this way it may be necessary for administrative roles to resolve manually any conflicts that arise. For example, the classification scheme may be altered in one back-up when compared to the other.*	
3218	The ERMS must allow administrative roles to indicate that records are no longer considered vital. This action must be recorded in the audit trail.	Y
3219	*For example a lease agreement or contract might expire and therefore no longer be considered vital.*	

5 Retention and Disposition

Note to reviewers: after considerable discussion, it has been decided to adopt the term "retention and disposition schedule" instead of "disposition authority". This decision is final.

ID	Text, Requirement & Rationale	Testable
478	**Retention and Disposition**	
479	A fundamental aspect of records management is the use of retention and disposition schedules to govern the retention and eventual fate of records from ongoing operations. Retention and disposition schedules define how long the records have to be kept by the ERMS, and how they may be disposed of. Requirements for retention and disposition schedules are listed in section 5.1; a formal definition is in the glossary.	

ID	Text, Requirement & Rationale	Testable
478	**Retention and Disposition**	
480	The processes that can take place at the date specified by retention and disposition schedules are described in subsequent sections. Requirements for review processes are listed in section 5.2, and requirements for transfer, export and destruction are listed in section 5.3.	
3696	**Note to reviewers: in the previous draft retention and disposition schedules could not be applied to sub-files. In response to numerous requests, that has been changed. Retention and disposition schedules can now be applied to sub-files.**	
482	As explained in section 2.2 under the heading Electronic File and Volume, records can be managed in classes, files, sub-files and volumes, as appropriate to the business requirement. According to circumstances, retention and disposition schedules apply to classes, files and/or sub-files and/or volumes. Retention and disposition schedules can also be applied to record types, for example to apply short retention periods to sensitive personal data, or to apply long retention periods to engineering drawings.	
4454	MoReq2 includes the concept of "disposal holds", which was not mentioned in the previous version of MoReq. Disposal holds are used in response to unexpected events to ensure that specified records are not destroyed. The common example is to ensure that records that are, or that may be, required as evidence in legal proceedings are not routinely destroyed as a result of a disposition decision.	

5.1 Retention and Disposition Schedules

ID	Text, Requirement & Rationale	Testable
483	**5.1 Retention and Disposition Schedules**	
2182	**Requirement**	
2199	The ERMS must allow administrative roles, and only administrative roles, to create and maintain retention and disposition schedules.	Y
2977	The ERMS must not limit the number of retention and disposition schedules.	P
3685	The ERMS should be able to arrange retention and disposition schedules in a hierarchical structure resembling the structure of general and organisation-specific retention and disposition schedules authorised by appropriate mandates.	
3709	*A hierarchical structure will facilitate the management of numerous retention and disposition schedules.*	
2953	The ERMS must allocate a unique identifier to each retention and disposition schedule when it is created.	Y
4446	The ERMS must allow a unique title be entered for each retention and disposition schedule when it is created.	Y
2951	The ERMS must maintain an unalterable history of changes and deletions (audit trail) that are made to retention and disposition schedules including the date of change or deletion, and user making the change.	Y
2960	The ERMS must ensure that any amendment to a retention and disposition schedule is immediately applied to all entities to which the retention and disposition schedule is allocated.	Y
3688	The ERMS must require an administrative role changing or deleting a retention and disposition schedule to enter a reason, and must store that reason in the audit trail.	
2978	*Changes to, or deletions of, retention and disposition schedules must be controlled carefully to minimise the risk of records being destroyed inappropriately.*	

ID	Text, Requirement & Rationale	Testable
483	**5.1 Retention and Disposition Schedules**	
2952	The ERMS must be capable of importing and exporting retention and disposition schedules.	P
2980	The ERMS must ensure that every class, file, sub-file and volume always has at least one retention and disposition schedule.	Y
2981	*This requirement is included to ensure that no entities are created without a retention and disposition schedule; and to improve usability.*	
3692	The retention and disposition schedule applied by default to every new class, file, sub-file or volume should be inherited from its parent.	Y
2982	*Where this is not possible (for classes at the top level of the classification scheme and if no inheritable retention and disposition schedule applies - see <ID 2988>) a default retention and disposition schedule should be applied.*	
4625	Every record stored directly in a class must always have one retention and disposition schedule assigned to it.	
4626	The retention and disposition schedule applied by default to any new record stored directly in a class (see <section 3.2 ID4218>) must be inherited from its parent class.	
2197	The ERMS must allow an administrative role to apply a retention and disposition schedule to any class, file, sub-file, volume or record type at any time.	Y
2983	*The phrase "at any time" means that an administrative role can replace a retention and disposition schedule or (if the system supports multiple retention and disposition schedules, see <ID2196>) apply an additional retention and disposition schedule to any class, file, sub-file, volume or record type. One example will be the replacement of a default retention and disposition schedule; another is the application of an additional retention and disposition schedule in response to a regulatory investigation. This may cause a conflict between retention and disposition schedules: see <ID2192>.*	
2969	The ERMS should be able to apply a default retention and disposition schedule to record types.	Y
2985	*This implies that record types can exist with no applied retention and disposition schedule. This is acceptable, as each individual record will have at least one retention and disposition schedule applied to it, because each record is held in a file and requirement <ID29980> mandates that at least one retention and disposition schedule is applied to each file.*	
2196	The ERMS must allow more than one retention and disposition schedule to be applied to any class, file, sub-file or volume. That is for more than one to be in force for the same class, file, sub-file or volume at the same time.	Y
2914	*This is required to manage real-life scenarios, which involve retention requirements arising from a range of mandates and business needs. This is illustrated by one example, chosen from many possible.* *In this example, a file has a single retention and disposition schedule, assigned for business reasons, as the records within it are not expected to be subject to legal or regulatory retention requirements. The retention and disposition schedule applying to this file also applies to many other files. At some point, it becomes apparent that it may be necessary to retain the file for a longer period than the current retention and disposition schedule allows, due to a business issue related to a safety case. At this point, it seems that the contents of the file may become subject to a regulatory control related to safety regulations; so a second retention and disposition schedule is applied to the file, taking this into account. At a later time, it may become apparent that the safety issue did not exist; in that event the second retention and disposition schedule can be removed, leaving the original one in place and active.*	

ID	Text, Requirement & Rationale	Testable
483	**5.1 Retention and Disposition Schedules**	
2195	The retention and disposition of every record must be governed by the retention and disposition schedule (s) associated with the class, file, sub-file, volume and record type to which the record belongs; and by any applicable legal hold(s) (see <ID2971>).	Y
2970	The ERMS must allow an administrative role to apply any retention and disposition schedule to any class, file, sub-file, volume or record type.	Y
2987	*Once a retention and disposition schedule is applied, it governs the retention and disposition of records associated with the entity to which it is applied (unless it is overridden by a different retention and disposition schedule.*	
2988	The ERMS must allow any retention and disposition schedule to be inherited down the hierarchy of the classification scheme, at the option of an administrative role.	Y
2989	*Whether or not a retention and disposition schedule is inherited can be selected by an administrative role using any appropriate means. MoReq2 does not prescribe how this is achieved. Possibilities include:* • *the option is selected when the retention and disposition schedule is created (in which case it applies whenever the authority is applied);* • *the option is selected whenever the retention and disposition schedule is applied (in which case it applies to all descendant entities);* • *the option is selected when an entity is created for it to inherit the retention and disposition schedule (s) of its parent.*	
2194	Each retention and disposition schedule must include: • a trigger event; • a disposition decision <ID 2191>; • a retention period <ID 2190>; • a reason.	Y
3699	Each retention and disposition schedule should include a: • a description; • a mandate.	Y
2991	*The mandate specifies the justification for the retention and disposition schedule. This is often a reference to a law, regulation or corporate policy.*	
2193	When the retention period applicable to some record(s) because of a retention and disposition schedule reaches its end, the ERMS must automatically initiate the processing of the disposition decision. This may mean that the decision is executed (subject to <insert references for checking before deletion>) or it may mean that action is required by an administrative role (see <ID2192>).	Y
2192	When the ERMS is initiating a disposition decision (as in <ID2193>), if any other retention and disposition schedule, with different retention period end and/or different disposition decision apply, then a conflict arises. If a conflict arises the ERMS must be able to automatically inform an administrative role to resolve the conflict by indicating which retention and disposition schedule is to take precedence.	Y
4449	*The words "must be able to…" are included because it is not required that administrative roles intervene in all situations. It is acceptable for the ERMS to resolve a conflict automatically; but it must be possible to configure the ERMS to require administrative intervention in the event of conflict.*	
2992	*A conflict can arise because* • *some retention and disposition schedule(s) indicate that disposition is to be initiated while some other(s) indicate the opposite;* *and/or* • *different retention and disposition schedules indicate different disposition decisions.*	

ID	Text, Requirement & Rationale	Testable
483	**5.1 Retention and Disposition Schedules**	
2993	*If the administrative role's resolution results in the records begin retained further, the resolution will need to include changing the retention and disposition schedules applying to the records, to ensure there is no conflict at the time of this action.*	
2994	*Administrative intervention may be required where it is not practical to define rules that correctly resolve these conflicts. For example:* • *two retention and disposition schedules, derived from different legal mandates may specify different retention periods. Normally, the decision will be to retain the records until the end of the later of the two end dates;* • *one retention and disposition schedule may specify a date by which certain records must be disposed of (typically because of data protection legislation mandate). If this date is earlier than the retention date of a conflicting retention and disposition schedule, then the decision will depend on the relative weight of the two mandates.*	
2191	The ERMS must allow at least the following disposition decisions (as defined in <ID 2194>) for each retention and disposition schedule: • retain permanently; • present for review; • destroy automatically; • destroy after approval from an administrative role; • transfer (to an archive or another repository, see glossary).	Y
2190	The ERMS must allow at least the following combinations of trigger events and retention periods (as defined in <ID 2194>) to be specified: • a specified date; • passage of a specified period of time after the class, file, sub-file or volume is opened; • passage of a specified period of time after the class, file, sub-file or volume is closed; • passage of a specified period of time since the most recent record has been classified to the class, file, sub-file or volume; • passage of a specified period of time since a record has been retrieved from the class, file, sub-file or volume; • passage of a specified period of time after a specified external event (which event is described in the schedule, and will be notified to the ERMS by an administrative role rather than being detected automatically by the ERMS) (for example, "…after contract signature"); • "permanent" to indicate long term preservation of the records.	Y
2915	*While the above is generally inclusive, it is possible that some organisations will want to impose additional activating events and/or additional retention periods.*	
2959	*Any number of external events can be linked to different disposition authorities.*	
3707	The ERMS should not limit the length of retention periods.	P
2189	The ERMS must support retention periods of time up to at least one hundred years for requirement <ID 2191>**.**	P
2916	*This maximum is suggested as an arbitrary period intended to avoid any practical limitation. While it is improbable that any ERMS will exist for one hundred years, a requirement of this nature will allow records to be transferred to future systems without the need to revise retention and disposition schedules.*	
2188	The ERMS must be able to restrict the management of the disposition process to administrative roles.	Y
2957	The ERMS must record in the audit trail and notify to an administrative role all automatic disposition actions**.**	Y

ID	Text, Requirement & Rationale	Testable
483	**5.1 Retention and Disposition Schedules**	
4041	The ERMS must automatically notify an administrative role when any review action becomes due.	Y
4042	The ERMS must allow an administrative role to delegate any notified review action to a reviewer role for action.	Y
2186	The ERMS must allow an administrative role to amend any retention and disposition schedule (apart from its unique identifier, see <ID2951>).	Y
2183	When an administrative role moves electronic files or records between classes of the classification scheme, the ERMS must offer the option to: • allow the retention and disposition schedule of the destination class to replace the existing retention and disposition schedule(s); or • enable an administrative role to select the appropriate retention and disposition schedule(s).	Y
4451	*This refers to moving records, as is permitted on an exception basis, in <IDxxxx>. On the rare occasions this functionality is used, administrative roles will need to take great care over the assigning or changing of retention and disposition schedules, especially for vital records.*	
2971	The ERMS must enable a disposal hold to be placed on a class, file, sub-file, or volume by an authorised user.	Y
4452	A disposal hold must not prevent any retention period from running and completing,	P
4453	*However, see <ID2971>.*	
2972	A disposal hold must prevent any entity subject to a disposal hold and any of its contents (descendant entities) from being deleted or being subject to any disposition decision.	Y
2997	*Deletion is described in section 9.3.*	
2973	The ERMS must restrict the removal of a disposal hold to an authorised user.	Y
3712	When an authorised user applies or lifts a disposal hold, the ERMS must capture and store the following information about it, at a minimum in the audit trail and preferably as metadata:	Y
3713	• the date the hold was applied; • the identity of the authorised user; • the reason for the hold.	
3714	The ERMS should allow an authorised user to apply several disposal holds, each specifying the same reason, to a group of classes, files, sub-files or volumes as a bulk operation.	Y
3715	The ERMS should allow the lifting of multiple disposal holds (citing the same reason) simultaneously, as a bulk operation, by an authorised user.	Y
3716	The ERMS should allow a class, file, sub-file or volume to be subject to multiple disposal holds simultaneously, either because they are applied to the entity and/or because they are applied to a higher-level entity. In either event the restrictions on disposition and other functionality imposed by disposal holds must remain in place until the last disposal hold affecting the entity is lifted.	Y
3717	The ERMS should allow an authorised user to search and report on all entities subject to a disposal hold.	Y
3718	The ERMS may allow an authorised user to set and reset a "reminder" that notifies the user of the existence of a specified disposal hold on a specified date.	Y

5.2 Review of Disposition Actions

ID	Text, Requirement & Rationale	Testable
523	**5.2 Review of Disposition Actions**	
524	In some environments, the retention and disposition schedules are used to govern disposition without a review. In others however, retention and disposition schedules trigger a review of the specified disposition action on a class or file etc. when the latter has reached the date or event specified in a schedule which applies to it. The review may consider metadata, contents or both in deciding on a further retention period, transfer to another system, destruction or combination of these, all as audited functions.	
525	The disposition of certain records is subject to laws and regulations. Reviews of disposition actions must be performed in a way which is consistent with these laws and regulations, with any appraisal policy and procedures set down for the organisation, and where appropriate in co-operation with (and sometimes exclusively by) responsible archival authorities. Further discussion of these issues is beyond the scope of this specification.	
2201	**Requirement**	
2211	The ERMS should automatically notify an administrative role of all retention and disposition schedules which will come into force in a specified period of time.	Y
2209	The ERMS must support the review process by presenting classes, files, sub-files and volumes to be reviewed together with their metadata and retention and disposition schedule information**.**	Y
2998	*In practice, this implies features for navigating forward, back etc. within and between files, and from/to the metadata for files and records.*	
2207	The ERMS must allow the reviewer to take at least any of the following actions for each class, file, sub-file or volume during review: • mark for destruction, immediately or at a future date <see 5.3>; • mark for transfer <see 5.3>, immediately or at a future date; • mark for a further review, immediately or at a future date; • mark for indefinite retention.	Y
2999	*This may be achieved by the application of different retention and disposition schedules, or by other means.*	
2963	The ERMS must automatically record the date of a review.	Y
2206	The ERMS must allow the reviewer to enter comments into the class, sub-file, volume, or file's metadata to record the reasons for the review decisions.	Y
2203	The ERMS must keep an unalterable history of all decisions taken by the reviewer during reviews, including reasons.	Y
2208	The ERMS should alert an administrative role if a conflict arises because a file that is due for destruction is referred to in a link from another file. It must pause the destruction process to allow the following remedial action to be taken: • confirmation by the administrative role to proceed with or cancel the process; • generation of a report detailing the files or record(s) concerned and all references or links for which it is a destination.	Y

5.3 Transfer, Export and Destruction

ID	Text, Requirement & Rationale	Testable
551	**5.3 Transfer, Export and Destruction**	

ID	Text, Requirement & Rationale	Testable
551	**5.3 Transfer, Export and Destruction**	
552	Organisations may need to move records from their ERMS to other locations or systems for archival or other purposes. This is referred to here as "transfer". Reasons for transfer may include: • permanent preservation of the records for legal, administrative or research reasons; • the use of devolved or external services for the medium term or long term management of the records.	
555	This action often results in the records being transferred to a different ERMS environment.	
3001	The term transfer is used even though, initially, only a copy is sent to the other location or system. The records originally residing in the ERMS are be retained and only destroyed upon verification that the transfer has been successful.	
4646	The term export, on the other hand, refers to the process of producing a copy of complete aggregations, files and records for another system, while the records remain on the originating system – the process does not delete them.	
3002	In effect the transfer process takes place in two stages - export of a copy with all associated metadata and audit trails with subsequent destruction of the original.	
557	In any event, the requirement is to execute the transfer, export or destruction in a controlled manner. In all cases, decisions must be taken on the metadata and audit trails at the same time as actions are carried out on the records they relate to.	
558	In this context "destruction" is different from "deletion". Deletion of records under other circumstances is covered in section 9.3.	
2213	**Requirement**	
2230	The ERMS must provide a well defined process to transfer records, together with their associated metadata and audit trail information to another system or to another organisation.	P
2229	Whenever the ERMS transfers any class, file, sub-file or volume, the transfer must include: • (for classes) all files in the class; • (for files) all volumes and sub-files in the file; • all records in all these files, sub-files or volumes; • all or selected metadata associated with all of the above; • all or selected audit trails for all of the above.	Y
4472	*Although the ERMS must be capable of exporting all metadata and audit trails, not all of these are always required by every target transfer system.*	
2922	The ERMS must be able to do either or both of the following when exporting or transferring any set of records: • export or transfer with the records the disposition authorities applied to those records, in a manner which allows the authorities to be re-applied to the records in the destination system; • print one or several reports showing the disposition authorities to be applied to each set of records, and the characteristics of these authorities.	Y
3003	The ERMS must be able to do either or both of the following when exporting or transferring any set of records: • export or transfer with the records the access controls for those records, in a manner which allows the controls to be re-applied to the records in the destination system; • print one or several reports showing the access controls applicable to each set of records, and the characteristics of these controls.	Y

ID	Text, Requirement & Rationale	Testable
551	**5.3 Transfer, Export and Destruction**	
2228	The ERMS must be able to transfer or export a file or the contents of a class in one sequence of operations, such that: • the content and structure of its electronic records are not degraded; • all components of an electronic record, (when the record consists of more than one component) are exported as one unit; • all links between the record and its metadata and audit trails are retained; • all links between classes, files, sub-files, volumes and records are retained so that they can be reconstituted in the receiving ERMS.	P
3357	When the ERMS is exporting volumes and/or files, if any of the volumes and/or files include pointers to records stored in other files (see chapter 3 <ID2111>) then the ERMS must export the complete record, not a pointer.	Y
3358	*This is required so as to make sure that there are no difficulties of pointer resolution between the exporting system and the receiving system.*	
2967	The ERMS must be able to transfer and export records in the format in which they were captured.	Y
4627	The ERMS must be able to transfer and export records in any format(s) into which records have been rendered.	Y
2226	The ERMS must also provide a utility or conversion tool to support the migration of records marked for transfer or export into approved transfer format(s).	Y
2918	*For example, an approved xml or other open format.*	
4473	*This requirement is to cover long retention periods where records must be automatically rendered into approved long-term preservation formats after a defined period of time without affecting the integrity and authenticity of the records.*	
2224	The ERMS must retain all files, records and other information that are being transferred, at least until confirmation of a successful transfer process.	Y
2919	*This is a procedural safeguard, to ensure that records are not destroyed before successful transfer-in is reported from the recipient.*	
4628	The ERMS must delete files, records and other information that are being transferred when it receives confirmation that the transfer process is successful, save for metadata that is retained as a stub.	
4629	*See <ID2217 below>.*	
2223	The ERMS should be able to export the entire contents of a class of the classification scheme in one sequence of operations, ensuring that: • the relative location of each file in the classification scheme is maintained, so that the file structure can be reconstructed; • sufficient metadata to rebuild the whole parent class branch is retained and moved with the contents of the class.	P
2221	The ERMS should provide the ability to add user-defined metadata elements required for archival management purposes to electronic files selected for transfer.	Y
2975	The ERMS must ensure that all renditions of a record marked for destruction are destroyed.	Y
4474	*Where the same record appears in more than one file (<ID2111> in chapter 3.4) then the record and its renditions should be removed from the file when it is destroyed but should not be finally deleted until all occurrences of the record have been destroyed.*	

ID	Text, Requirement & Rationale	Testable
551	**5.3 Transfer, Export and Destruction**	
2217	The ERMS must have the ability to retain a metadata "stub" (see Glossary) for: • classes; • files; • records stored directly in a class; which have been destroyed or transferred.	Y
3669	*In some environments it is desirable to retain information about records which have been destroyed. The metadata in question should include at least the date of acquisition and all the metadata relevant to identify uniquely each record and its relations to the classification scheme and the filing plan. See the MoReq2 metadata model.*	
2216	The ERMS must allow an administrative role to specify a subset of class, file and record metadata which will be retained for files which are destroyed or transferred, to constitute the metadata stubs.	Y
2923	*This is so that the organisation can still know what records it has held and the dates they were destroyed or disposed of, without incurring the overhead of keeping all the detailed metadata for files and records.*	
2215	The ERMS must allow files and records to be exported more than once.	Y

6 Capturing Records

ID	Text, Requirement & Rationale	Testable
596	**6 Capturing and Declaring Records**	
601	**Overview**	
602	This chapter covers requirements relating to the process of capturing records into an ERMS. The first section (6.1) covers the standard capture process. The following section (6.2) covers the bulk import of records from other systems. Section (6.3) describes considerations for particular kinds of objects; and this is followed by a section devoted to e-mail because of its particular importance (6.4). Section 6.5 concerns record types and section 6.6 covers integration with scanning and imaging systems.	
597	**Terminology**	
4645	**Note to reviewers: the paragraphs about terminology in this section of the last draft generated many comments, some contradictory with others. Plainly there is no single formulation of the key terms here that will satisfy everybody. We have significantly revised terminology in this section, aiming to clarify without introducing unduly contentious definitions.**	
4466	The term "capture" is used in this and other chapters of MoReq2. The term is used with its natural English language sense, in an information management/information technology context. In this context, "capturing" information means saving it in a computer system. This is consistent with the archival meaning of "capture", given as "the act of recording or saving a particular instantiation of a digital object" in the InterPares 2 Project Terminology Database (see footnote).	
598	**Insert footnote:** See http://www.interpares.org/ip2/ip2_terminology_db.cfm	
4465	It follows that ERMSs can capture a range of information. An ERMS can capture records, metadata, and in some cases documents, among others.	

ID	Text, Requirement & Rationale	Testable
596	**6 Capturing and Declaring Records**	
4176	The fact that an ERMS can (in some cases) capture documents as well as records leads to the inevitable conclusion that the term "capture" is imprecise, because capturing a record involves more processes than capturing a document that is not a record. For example, capturing a record includes the processes of classification, registration, and locking against change whereas this is not necessarily the case for documents. Perhaps for this reason, for records the term "declare" is used synonymously with "capture"; however, the term "declare" can apply to a document that starts outside the ERMS, or to a document that has already been captured as a document by the ERMS.	
599	While this lack of precision is undesirable, it has little or no negative impact on the clarity of MoReq2.	
600	More formal definitions are given in the Glossary in section 13.1.	

6.1 Capture

ID	Text, Requirement & Rationale	Testable
603	**6.1 Capture**	
605	Electronic documents that are made or received in the course of business processes originate from both internal and external sources. The electronic documents will be in various formats, be produced by different authors and may be received either as single documents or as documents comprised of several components (see glossary for definition of "component" in the context of MoReq2).	
2827	Some records are created within the organisation, in the course of its business processes. Others are received through various communication channels e.g. electronic mail, facsimile, letter post (optionally to be scanned), by hand, and at variable arrival rates and volumes. A flexible capture system with good management controls is required to capture documents so that their diverse requirements are addressed.	
2232	**Requirement**	
2247	The ERMS capture process must provide the controls and functionality to allow users to: • capture electronic records regardless of file format, method of encoding or other technological characteristics, with no alteration of their content; • ensure that the records are associated with a classification scheme; • ensure that the records are associated with one or more files.	P
3747	*File format is defined in the Glossary. The requirement to be able to capture any file format.*	

ID	Text, Requirement & Rationale	Testable
603	**6.1 Capture**	
2877	*The requirement to capture records in any file format is not intended to be testable, and it does not imply that the ERMS needs to be able to make presentations (see Glossary) of all possible formats. MoReq2 therefore does not list the kinds of formats that may be captured, as formats vary over time with the evolution of software. However, for the avoidance of doubt, the kinds of records to be included can be diverse; they might include, for example, the following kinds of records frequently used in office settings:* • *output from desktop applications such as office suites;* • *emails (see section 6.x);* • *audio;* • *databases;* • *portable document formats;* • *scanned images;* • *video;* • *web pages.*	
2878	*In some situations, the ERMS may also need to capture other kinds of record such as:*	
2843	• *compressed files (sometimes referred to as "archives", applying an IT meaning of the term);* • *electronic calendars;* • *electronic forms;* • *geographical information system data;* • *information from other computer applications e.g., accounting, payroll, computer aided design;* • *instant messaging systems;* • *multimedia documents;* • *records of web-based transactions;* • *records which include links to other records;* • *software source code and project documentation;* • *structured data (e.g. EDI transactions);* • *webcasts;* • *wikis.*	
2879	*These lists are not complete.*	
2254	The ERMS must not impose any practical limit on the number of records which can be captured in any class, file, sub-file or volume, nor on the number of records which can be stored in the ERMS.	P
4486	*Large numbers of records in volumes etc. will tend to make the system difficult to use in some settings, and so is not generally advisable. This requirement is intended to allow for situations in which large numbers are unavoidable, such as some transactional environments.*	
2253	When capturing a record made up of several components (see Glossary), the ERMS must capture all of its components.	P
2235	When capturing electronic records that have more than one component, the ERMS must allow the record to be managed as a single unit, retaining the relationship between the components, and retaining the record's structural integrity.	P
2725	*Examples of such records are:* • *web pages with embedded graphics;* • *an e-mail with an attachment;* • *a word-processed document with an embedded spreadsheet.*	

ID	Text, Requirement & Rationale	Testable
603	**6.1 Capture**	
4635	*In some cases, the components will be related by links that do not work if simply copied t into the ERMS repository. For example, many web pages contain links to graphics and other objects with addresses (urls) that are external to the repository; and linked spreadsheets typically contain links to addresses (operating system filenames) external to the repository. See next requirement.*	
4636	When capturing electronic records that have more than one component, and which are in a file formats required by the organisation, the ERMS should modify the record if necessary to preserve the ability to present it; this is likely to mean that the ERMS changes the internal references (links) within some of the components.	Y
4637	*Making such changes is contrary to the general principle of not changing the content of records, but is unavoidable if records that include components etc. are to be stored in their original formats without losing all functionality and fidelity. The changes will generally be acceptable so long as the changes are recorded in the ERMS audit trail (see next requirement). An alternative approach involves rendering the record into some other file format (such as PDF/A) that preserves the static appearance; see <section 11.7 requirement ID4026>.*	
4638	When the ERMS changes references within records, it must record automatically all details of the changes made in its audit trail.	Y
2881	The ERMS must automatically capture the file format (see Glossary), including its version of each component when it is captured and must store it in the metadata of the component or record.	P
4492	*This is required to support the digital preservation of records – their accessibility over time. See section <11.7>.*	
2828	*Some information about file format is usually implicit in the component's filename extension, e.g. ".htm" or ".pdf"; and on occasion it is ambiguous, e.g. ".doc" can specify several unrelated formats. However, the extension alone frequently does not indicate the file format version. This will be acceptable in many cases, though it may not suffice in cases where long-term preservation is needed, or where precision is needed (for example, precision of colour space).*	
2882	*File formats are numerous and are subject to frequent change. It therefore is not realistic to expect an ERMS to capture information for all file formats. It is therefore acceptable for the ERMS to:* • *specify a list of file formats that can be recognised;* • *rely on reference to an established file format registry – preferably one designed specifically to support digital preservation.* *In either case, the using organisation needs to satisfy itself that the range of file formats included is sufficient for its preservation requirements.*	
2880	The ERMS record capture process must validate the values of metadata entered into the ERMS when records are being captured, at a minimum according to the rules in the MoReq2 metadata model.	Y
4487	*See also <ID2236> in this section.*	
2830	The ERMS must allow users to capture an electronic record even if the generating application is not present.	Y
2831	*For example a user may receive a project plan and a CAD/CAM drawing as attachments in an e-mail. If the user does not have access to the project plan or CAD/CAM applications, then the user may not be able to view the attachments. Regardless of this, the user should be able to capture the attachments as records in the ERMS. The ERMS may provide "viewer" software that allows the user to view these records; this is not required by MoReq2.*	

ID	Text, Requirement & Rationale	Testable
603	**6.1 Capture**	
2832	The ERMS must be able to capture metadata about records consistent with the MoReq2 metadata model.	Y
2833	The ERMS should be able to capture automatically values from fields defined by an administrative role within the specified document types, using these values automatically to populate metadata elements as specified in the MoReq2 metadata model.	Y
4493	*The functionality needed for this requirement applies only to specific kinds of electronic objects, for example letters produced using a specified template and a specified word processor.*	
2760	*Many documents including some office documents and .pdf files include user-configurable metadata elements. It should be possible to configure the ERMS to capture automatically the values of these elements and retain them with the record.*	
2245	The ERMS must allow the capture of all metadata elements specified at system configuration, and must retain them with the electronic record in a persistently-linked relationship at all times.	Y
4494	The ERMS should allow users who wish to capture a record but who are unable to provide all the mandatory metadata values for it to store it temporarily in the ERMS.	Y
4495	*This implies exception reporting and progress monitoring. MoReq2 does not specify how this is achieved.*	
2244	The ERMS must ensure that the values of some elements of the metadata of the electronic record can only be updated by authorised users and administrative roles, consistent with the rules in chapter 12.	Y
2845	The ERMS must ensure that all records are assigned to at least one class, file (or its sub-file if appropriate), as appropriate, when it is captured.	Y
2234	The ERMS should support automated assistance in capturing electronic documents, by automatically extracting as much metadata as possible, for as many kinds of document as possible.	N
2726	*The rationales for this requirement are to minimise the amount of data entry performed by users and to increase the accuracy of metadata. The metadata elements involved, and the kinds of documents for which this is possible, will depend on the environment.*	
2242	The ERMS must support automated assistance in the capture of outgoing and internal office documents (e.g. memoranda or word-processed letters in a specified layout and file format) as records, by automatically extracting the following metadata from them: • document date (as in the body of the document); • recipient(s); • any copy recipient(s); • subject line (title); • author(s); • internal reference; to the extent that these are present.	Y
2886	*MoReq2 does not specify the software or formats for office documents or e-mail. The metadata extraction may be achieved by locating metadata within the record, by using a template to identify the metadata and populate a blank document, or by any other means.*	
2241	The ERMS must record the capture date and time of a record both as metadata and in the audit trail.	Y
2723	*If the date and time are part of the unique identifier of the record, and as long as they can be explicitly extracted from this number, it is not necessary to store the date and time separately.*	

ID	Text, Requirement & Rationale	Testable
603	**6.1 Capture**	
4497	*MoReq2 does not specify the accuracy of the time needed. Most ERMSs record time to an accuracy of one second or better.*	
4498	*Some legislative frameworks call for time stamping to be performed against a certified device or authority. Where this is the case it should be accommodated in a chapter zero.*	
2240	For every captured record, the ERMS must be able to present on-screen a registry entry, including the metadata specified at configuration time.	Y
2724	*The metadata specified at configuration time may consist of any or all elements from the relevant section of chapter 12.*	
2836	The ERMS must ensure that all mandatory metadata is present for every captured record.	Y
2835	During capture of a record the ERMS must prompt the user to enter any required metadata that has not automatically been captured.	Y
2807	The ERMS must support the assignment of multiple keywords (or key terms) to each class, file, sub-file and record.	Y
4500	*MoReq2 does not require the ability to assign keywords to volumes.*	
4499	The ERMS should allow an administrative role to configure whether keywords are mandatory or optional, at configuration time, for each of classes, files and sub-files.	Y
2809	The ERMS must allow more than one file to be created using the same combination of keywords.	Y
4217	The ERMS must provide a capability for the keywords to be picked from, or validated against, controlled vocabularies (or lists of permitted terms).	Y
4501	*For example, by means of a pick list.*	
2813	Where a controlled vocabulary of keywords takes the form of an ISO 2788-compliant or ISO 5964-compliant thesaurus, the ERMS should allow users who are creating metadata values use the full features of the thesaurus, such as broader, narrower and related terms and synonyms in a manner that is fully integrated with the ERMS.	Y
2239	The ERMS must allow entry of further descriptive and other metadata at the time of capture and/or at a later stage of processing.	Y
2837	The ERMS must enable the user to assign a title to an electronic record upon registration, allowing this title to differ from the operating system filename or subject line.	Y
2842	The ERMS must warn the user if an attempt is made to capture an object with a title which already exists in the same file or to re-title an object with a title which already exists in the same file.	Y
3875	See also <C11 ID4087>.	
2838	The ERMS must be able to reserve the ability to amend the title of an electronic record for an administrative role or other authorised user.	Y
4503	*This facility can be used or not used, at the option of the organisation.*	
2238	When a user is capturing a document that has more than one version, the ERMS must allow the user to choose at least one of the following: • declare all versions as one record; • declare one specified version as a record; • declare each version as an individual record.	Y

ID	Text, Requirement & Rationale	Testable
603	**6.1 Capture**	
2237	The ERMS should be able to provide automated support for decisions on the classification of electronic records to files by means of at least one of the following: • making only a subset of a classification scheme accessible to a user or role; • suggesting the files used most recently by that user; • suggesting the files used most frequently by that user; • suggesting files by inferences drawn from record metadata elements (for example, significant words used in the title or e-mail subject line); • suggesting files by inferences drawn from the record contents.	P
2236	The ERMS should allow the process of capturing a record to be completed by a more than one user.	Y
2887	*The ERMS should allow the capture process to be divided between users; typically this will mean that one user enters some metadata then passes the electronic record to another user, who enters the remaining metadata and classifies the record.*	
4394	The ERMS should provide simple workflow facilities to enable simple routing for checking and approving a document before capture, recording the decisions taken, who took them, and allowing a reason to be entered by each.	Y
4395	*Note that this requires only basic workflow features. It intentionally stops short of the full workflow features described in chapter 10.*	
2889	Where possible, the ERMS should issue a warning if a user attempts to capture an e-mail record which has already been captured into the same file.	Y
4506	*MoReq2 does not define how the e-mail is identified; however, the internet message ID may be suitable.*	
4504	*There are several cases in which this is not logically possible, for example where the e-mail record has been captured into a file to which the user is denied access.*	
2233	Where possible, the ERMS should issue a warning if a user attempts to capture a record (other than an e-mail, as this is dealt with by <ID 2889 above>) that has the same values of identifying metadata as another record which has already been registered in the same file.	Y
2890	*The identifying metadata for this requirement is:* • *Title;* • *Date;* • *Author;* • *Addressee.*	
2165	Where possible and appropriate, the ERMS should be able to provide a warning if an attempt is made to capture a record which is incomplete or inconsistent in a way which will compromise its future apparent reliability.	N
3198	*For example, a purchase order without a valid electronic signature or an invoice from an unrecognised supplier.*	

6.2 Bulk importing

ID	Text, Requirement & Rationale	Testable
639	**6.2 Bulk importing**	

ID	Text, Requirement & Rationale	Testable
639	**6.2 Bulk importing**	
640	Records may reach the ERMS in bulk in a number of ways. For example: • a bulk transfer from a compatible EDMS; • as a single compatible data file containing a series of records of the same type (e.g. daily invoices); • from a compatible scanning or imaging system; • records from a hierarchy of operating system folders. The ERMS needs to be able to accept these, and must include features to manage the capture process and maintain the content and structure of the imported records.	
4507	During bulk import the ERMS needs to capture the same information as the normal capture process – namely the records themselves and their metadata. It also needs to classify the records – this may involve capturing the definition of extensions to its classification scheme (see <section 3.1 ID2677> - and it may additionally involve capturing audit trail information. Finally, bulk import needs to allow for the processing of exceptions and errors.	
2248	**Requirement**	
2251	The ERMS must provide the ability to capture transactional records generated by other systems. This must include: • supporting predefined batch file transaction imports; • providing editable rules to customise the automatic capture of the records; • validation to maintain data integrity.	P
2250	The ERMS must provide facilities to manage input queues.	Y
2846	The ERMS must be able to capture automatically the metadata associated with records during a bulk import (allowing for manual input of missing or incorrect metadata).	P
2891	Where the ERMS captures the metadata of some record(s) during import, it must validate it using the same rules as would be used for the manual capture of the records(s). Where this validation process finds errors (such as absence of mandatory metadata, or format errors) it must bring these to the attention of the user performing the importation, in all cases identifying the metadata involved, and recording errors and actions in the audit trail.	Y
2892	*In ideal cases, the record(s) being imported will have metadata that complies fully with the metadata model. In other cases, the metadata may be non-compliant. In these cases, several outcomes are possible; MoReq2 does not mandate any one outcome. Possible outcomes include:* • *The entire importation is cancelled;* • *Importation of the record that has non-compliant metadata is cancelled;* • *The user is required to choose between correcting the error and cancelling importation of the affected class;* • *The data is imported as a temporary incomplete record (this resembles the requirement that capture can be divided between users, see <section 6.2 ID2236>).*	
2849	The ERMS must be able to import audit trail records that show the history of the imported record(s).	Y
2893	The ERMS must not import audit trail records into its audit trail; it must store imported audit trail records separately.	
3748	*The imported audit trail records must be maintained separately so as to avoid producing a mechanism that allows administrative roles to change or compromise the integrity of the audit trail. MoReq2 does not specify how this is achieved; it may involve storing the imported audit trail as a record alongside the imported records, or as a separate entity recognised as an audit trail imported from another system.*	

ID	Text, Requirement & Rationale	Testable
639	**6.2 Bulk importing**	
2850	The ERMS must enable an administrative role to (optionally) set the ERMS to close classes, files and volumes automatically after they have been imported.	Y
2851	*For example, on the merger of two organisations it may be necessary to close down branches of the structure so that records can no longer be added to them.*	

6.3 Types of Document

Note to reviewers: all the requirements from this section have been included elsewhere, mainly 6.2. Accordingly this section has been deleted. This heading is retained in this draft for numbering purposes only.

6.4 e-Mail Management

ID	Text, Requirement & Rationale	Testable
675	**6.4 e-Mail Management**	
4508	**Definitions**	
4512	As a verb, "e-mail" refers to a mechanism for transmitting messages between "agents" (in this context, the term" agent" has a precise technical meaning; more detail is not required for an understanding of MoReq2).	
4513	The standard protocol used for e-mailing is defined by the Network Working Group requests for comment RFC 2821 and RFC 2822. MoReq2 uses RFC 2821/RFC 2822 as the basis of its working definition of "e-mail".	
4509	As a noun, "e-mail" is usually used to refer to a document captured from an agent that contains the complete data of a single e-mail transmission. However, although RFC 2822 defines the syntax for e-mail transmissions, there are no standards that define the data format that should be used when e-mail transmissions are captured as documents.	
4510	In other words, even though e-mail applications from different suppliers can freely transmit messages between one another (because they observe the e-mail protocols defined in RFC 2821/ RFC 2822) it is not possible to capture an e-mail transmission from one e-mail application as a document and guarantee that another e-mail application will be able to read it back, as each e-mail supplier observes its own proprietary format(s) for capturing e-mail. Likewise, the automated extraction of metadata from messages cannot be based on standards.	
4511	**Use and issues**	
676	e-Mail is used for sending documents (in the form of messages and as attachments) within and between organisations. The characteristics of e-mail management software (in particular the lack of standardisation for formats explained above), combined with user attitudes towards e-mail, can make it difficult to apply records management functionality to e-mail. Organisations need to be able to enforce procedures and management controls to: • capture all inbound and outbound e-mails and attachments; and/or to: • capture e-mails and attachments according to pre-defined rules; and/or to: • provide users with the capability of capturing selected e-mails and attachments	
4175	In European member states the legal ownership of e-mail is unclear and in some cases automatic capture of e-mails into an ERMS may be inappropriate. Where this is held to be the case the latter two options should be considered for configuration.	

ID	Text, Requirement & Rationale	Testable
675	**6.4 e-Mail Management**	
2860	Furthermore, e-mail has become the default means of communication for many organisations and an important means for others. As such, much e-mail traffic is ephemeral. Each organisation needs to decide which of the above approaches represents the most appropriate compromise for their situation:	
680	• The first option results in the capture of any ephemeral e-mails as well as those that are meaningful records; • The second option relies on successfully configuring appropriate rules and filters; • The third option requires the users to assess the relevance and importance of items, and there is a risk that they will not all do so reliably.	
2863	MoReq2 allows for ERMS support for all three approaches. The procedures and management controls are beyond the scope of MoReq2.	
2259	**Requirement**	
4518	Whenever an e-mail is captured, the ERMS must by default capture it in a format that retains its header information.	Y
2894	The ERMS must support the capture of e-mails in an integrated way, such that the capture can be performed by a user from within the e-mail application, without the user needing to switch to the ERMS.	Y
2895	*MoReq also permits, but does not require, the capture of e-mails in other, less closely integrated ways.*	
2262	It must be possible to configure the ERMS at configuration time so that it operates in one of the following ways when a user sends an e-mail: • it automatically captures the e-mail; • it determines whether to capture the e-mail according to pre-defined rules; • it automatically prompts the user, giving the user an option to capture the message-mail; • it takes no action (and thus relies on the user to initiate a capture if appropriate).	Y
2934	*Regardless of which way is chosen, it is acceptable for the ERMS to require the user to classify records manually and enter some metadata manually.*	
2935	It must be possible to configure the ERMS at configuration time so that it operates in one of the following ways when an ERMS user receives an e-mail: • it automatically captures the message, unless it has already been captured; • it determines whether to capture the e-mail according to pre-defined rules; • if the e-mail has not already been captured it automatically prompts the user, giving the user an option to capture it; • it takes no action (and thus relies on the user to initiate a capture if appropriate).	Y
2936	*Regardless of which way is chosen, it is acceptable for the ERMS to require the user to classify the record manually and enter metadata manually.*	
2261	The ERMS must be tightly integrated with the e-mail system to enable users to capture e-mails into the ERMS from within the e-mail client.	Y
2862	*Close integration is essential for effective use of an ERMS. For example the user should be able to "drag and drop" from the e-mail client into the ERMS, or choose a "capture" command from within the e-mail client. The essence of this requirement is that the user must not have to switch to the ERMS application to capture e-mails.*	

ID	Text, Requirement & Rationale	Testable
675	**6.4 e-Mail Management**	
4415	The ERMS must support automated assistance in the capture of outgoing and incoming e-mails, with and without attachments, as records, by automatically extracting the following metadata from them: • e-mail date sent (and in some settings, time); • recipient(s); • any copy recipient(s); • subject line (title); • sender; • embedded electronic signature; • Certification Authority; • to the extent that these are present.	P
4496	*This requirement specifies the capture of "sender" for e-mail messages. This not always the same as the author, for example when a secretary sends a message on behalf of an executive. The capture of "sender" is specified here as a conscious compromise, it being impossible to reliably capture the author automatically. Organisations should consider the need for manual procedures to ensure the correctness of the author metadata.*	
4075	Users should be able to allocate an e-mail record to a sub-file, file or class by dragging it from an e-mail client (technically, a Mail User Agent) to a specified sub-file, file or class in the ERMS.	Y
4516	*The class, file or sub-file can be represented in the e-mail client window or in a separate window.*	
2739	The ERMS must allow a user to choose how to capture an e-mail message with attachment(s) as: • the e-mail message only, without attachments; • the e-mail with its attachment(s), as one record made of linked components; • the attachment(s) only, each or any as individual records.	Y
2937	*This applies to sent and received messages.*	
4517	*The last of these three options results in attachments being captured without the context of the e-mail with which they were transmitted.*	
2744	Where an e-mail and its attachment(s) are captured at the same time but as separate records, the resultant records should be linked automatically by the ERMS.	Y
2939	*The ERMS should allow a user to navigate the cross-reference link between the records so as to discover each of the attachment records from the e-mail record and the e-mail record from any of the attachment records.*	
2938	When capturing an e-mail message, the ERMS must by default populate the Title metadata with the "subject" field of the message.	Y
2740	The ERMS must allow a user who is capturing an e-mail message to edit the record title.	Y
2940	*This is intended to allow users to correct inappropriate or to clarify imprecise e-mail titles, or to make the titles more meaningful.*	
4518	*The e-mail title is separate from the subject line (title) of the e-mail; the latter will remain as part of the message regardless of the content of the e-mail title.*	
2859	If a user captures an e-mail delivery status notification report (where these are supported) for an e-mail which has been captured as a record, the ERMS should be able to link the two automatically.	Y

ID	Text, Requirement & Rationale	Testable
675	**6.4 e-Mail Management**	
2941	*Examples of delivery status notifications are non-delivery reports and delivery confirmations. The link should allow a user to navigate between the records so as to discover each of the notifications from the e-mail record and the e-mail record from any of the notifications.*	
2742	The ERMS must enable the automatic capturing of metadata belonging to e-mails and their attachments as outlined in chapter 12.	Y
4470	The ERMS must allow "date sent" and "date received" metadata to be entered manually.	
4471	*This is to allow for situations in which the dates held in the e-mail message are not appropriate for the business setting.*	
2746	A user must be able to capture into the ERMS, in a single operation, several manually-selected e-mails as: • one record; or as • a set of records, one per e-mail; at the user's option.	Y
4520	The ERMS should be able to identify automatically and capture all the e-mails related to an e-mail specified by a user, in a single operation, capturing them as: • one record; or as • a set of records, one per e-mail; at the user's option.	Y
4521	*RFC 2822 Section 3.6.4. "Identification fields" describes how the optional SMTP header fields "References:" and "In-Reply-To:" can be used in conjunction with the "Message-ID:" field to identify related e-mail messages, sometimes referred to as the 'thread of the discussion.'*	
3704	The ERMS must allow a user who is capturing an e-mail message in a proprietary format to save in multiple, including open, formats	Y
3705	*It may be useful for an EDRMS to enforce saving criteria on e-mails based on the retention and disposition schedule. Folders with a short retention period could be stored in a proprietary format, but those with longer schedules could be saved into an open format.*	
2260	Whenever address fields captured from an e-mail header appear in the metadata of an e-mail record, the ERMS must ensure that it captures the optional "display name" (if present) of any mailbox listed as well as the "address-spec" address;; for example, 'Jan Schmidt' rather than 'js97@xyz.int'.	Y

6.5 Record Types

ID	Text, Requirement & Rationale	Testable
2050	**6.5 Record Types**	
2051	Record Type describes characteristics of records that defines characteristics that are not (and usually cannot be) defined in the classification scheme. This can include specific: • metadata attributes; • retention requirements; • access controls; • kind of document (e.g. contract, CV, disciplinary report).	

ID	Text, Requirement & Rationale	Testable
2050	**6.5 Record Types**	
4654	A record's record type usually corresponds to the document type of the document from which the record was made.	
3749	**Requirement**	
2709	The ERMS must support the definition and maintenance of record types.	Y
2751	All records in the ERMS must have one record type.	Y
2710	The ERMS must restrict the definition and maintenance of record types to an administrative role.	Y
2897	The ERMS must allow an administrative role to restrict the creation of records of specified record types to specified groups of users, based on their business needs.	Y
2712	The ERMS must allow an administrative role to define one record type as the default record type, which can be used by all users who are allowed to capture records.	Y

6.6 Scanning and Imaging

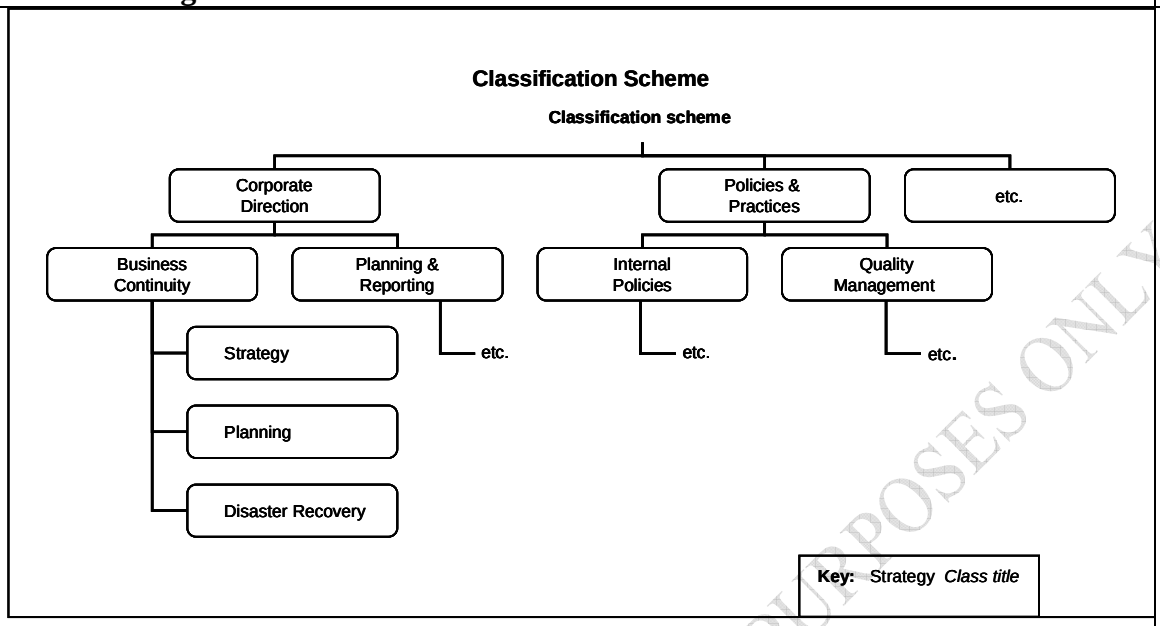
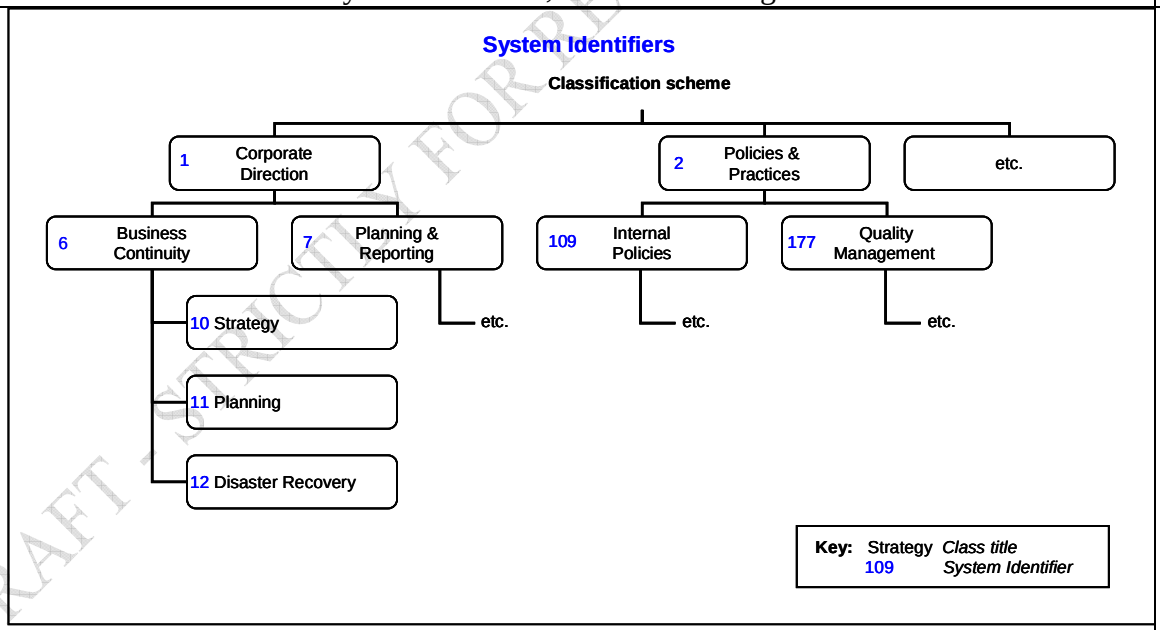
ID	Text, Requirement & Rationale	Testable
2056	**6.6 Scanning and Imaging**	
2057	When planning for the implementation of an ERMS, physical records in the form of paper or microform often need to be considered.	
2903	There are two main issues: • existing records that are held on paper or microform and may need to be referred to in conjunction with electronic records; • documents on paper that continue to be received or created by the organisation, but which the organisation wishes to hold as electronic records in the ERMS.	
2910	This section deals with the scanning (imaging) of paper-based and microform, documents, so that they can be captured into the ERMS as electronic records.	
2909	Scanning can be organised in the following ways: • centralised; • local or workgroup; • outsourced or subcontracted; or in any combination. These ways are described briefly below.	
2908	Centralised scanning is most appropriate for high-volume capture, typically using fast scanning equipment specifically designed for bulk input, together with specialist scanner operators.	
2907	Local or workgroup scanning takes place close to the receiving users and is appropriate for low-volume activity, or where the person doing the scanning needs a knowledge of the business, or when dictated by the geographic distribution of the organisation. This typically uses scanners with lower capacity and speed.	
2906	Outsourced or subcontracted scanning - this can be considered for a number of reasons: • where there is a large amount of scanning to be done as a one-off exercise; • where sufficient human and/or equipment resources are not available within the organisation ; • where the scanning is not site-dependent.	
2905	The rest of this section sets out key requirements to be considered in provision of an integrated ERMS and scanning solution. The requirements apply only where scanning facilities are part of the ERMS; however, many can be interpreted for use when scanning is outsourced.	

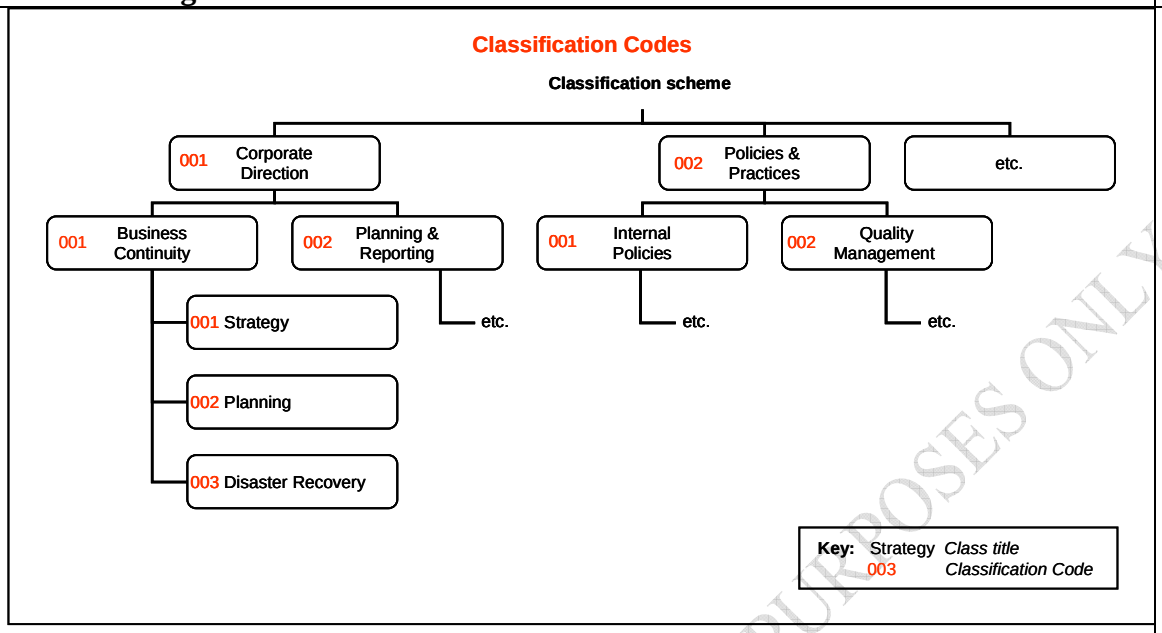
ID	Text, Requirement & Rationale	Testable
2056	**6.6 Scanning and Imaging**	
2904	**Requirements**	
4117	The ERMS must be capable of integration with at least one scanning solution.	Y
4118	*The scanning solution provides the interface with the scanning equipment and allows the operator to perform several processes related to scanning such as rotating, descreening and despeckling.*	
4119	The ERMS scanning feature must be capable of saving images in standard formats, including, but not limited to: • TIFF; • JPEG (only required if colour is supported); • PDF/A.	Y
4120	The ERMS scanning feature must be capable of saving images in monochrome at different resolutions.	Y
4121	*Ideally the scanning feature should provide a menu of options, programmable for the input of different types of document.*	
4522	The ERMS scanning feature should be capable of saving images in colour or greyscale and at different resolutions.	Y
4131	The ERMS scanning feature must be capable of handling standard paper sizes, including, but not limited to: • A4; • A3.	Y
4122	The ERMS scanning feature should have Optical Character Recognition (OCR) functionality.	Y
4123	*OCR functionality produces text from a scanned image. Some kinds of OCR are sometimes referred to as Intelligent Character Recognitions, or ICR. For simplicity, MoReq2 refers to both as OCR.*	
4138	Where the ERMS includes OCR functionality the ERMS should be capable of managing the scanned image and the text resulting from the OCR as a single record.	Y
4488	*In other words, the OCR text should be regarded as metadata of the record rather than as a record in its own right.*	
4489	*MoReq2 does not require that users be able to view the OCR text, as its purpose is to allow full text searching (see next requirement).*	
4490	Where the ERMS includes OCR functionality it should support full text searching based on the text.	Y
4124	The ERMS scanning feature should be capable of recognising and capturing individual documents in a bulk scanning process.	Y
4125	*MoReq2 does not specify how this should be done. Common solutions rely on the recognition of patch codes, barcodes or blank sheet inserts.*	
4126	The ERMS scanning feature must be capable of automatically sending scanned images to a queue for after scanning and in between each process.	Y
4523	*For example, indexing, quality assurance.*	
4132	The ERMS scanning feature should include a software viewer for inspection of the scanned images.	Y
4524	The ERMS should be able to display thumbnails of scanned images as an aid to navigation and searching.	Y

ID	Text, Requirement & Rationale	Testable
2056	**6.6 Scanning and Imaging**	
4127	The ERMS scanning feature should log each scanning session with the following details: • user login; • workstation identifier; • time and duration; • session identifier; • batch identifier(s); • number of documents (if applicable); • number of images.	Y
4133	The ERMS scanning feature should be able automatically to capture relevant metadata when scanning zoned forms.	Y
4525	*A zoned form is one which includes areas defined in the scanning software as containing data to be scanned. The information outside the defined zones is not scanned, thus reducing image size and reducing storage and bandwidth requirements.*	
4128	Where the ERMS scanning feature includes automatic capture of metadata it should be able to interpret this information for automated classification.	Y
4129	*This feature is especially useful in Casework environments, where paper records frequently bear case identifiers that contain sufficient information to classify the record - see chapter 10.X <ID2058>.*	
4136	The ERMS should be capable of the bulk import of scanned images and their metadata.	Y
4137	*See chapter 6.2 for further requirements regarding bulk import.*	

7 Referencing

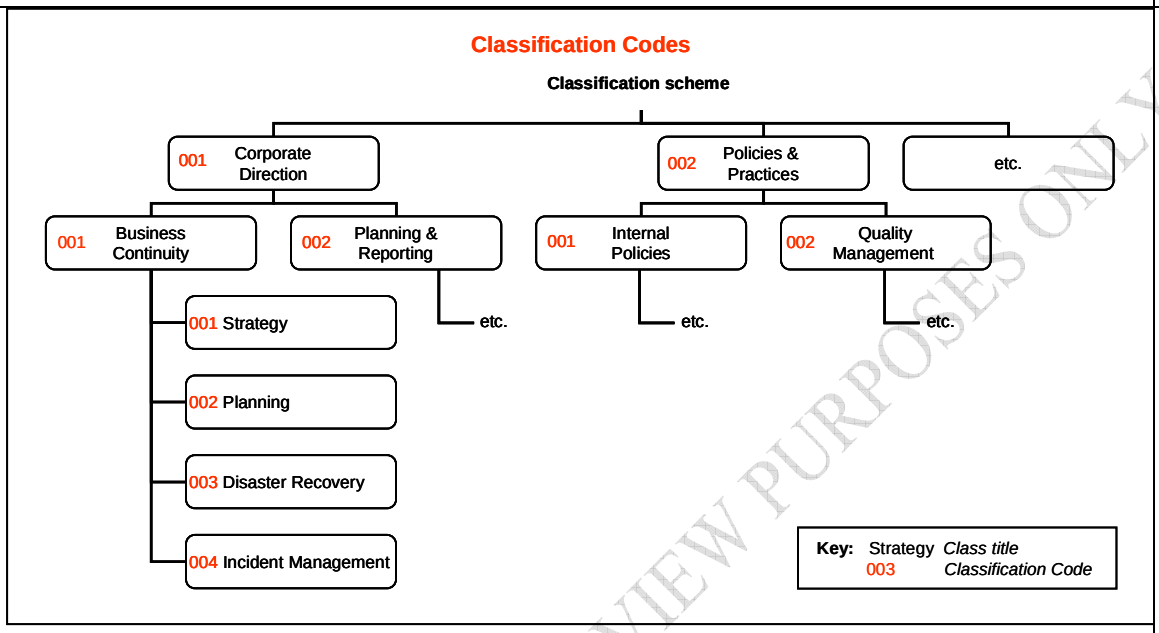
ID	Text, Requirement & Rationale	Testable
690	**7 Referencing**	
691	All of the entities stored in the ERMS repositories (classes, files, sub-files, volumes, records etc.) need identifiers. These identifiers are needed to: • Allow the software to process the entities; • Allow users to retrieve, refer to, and use, the entities.	
3931	MoReq2 uses the following terminology to describe these identifiers: • An identifier required for software usage is called “System Identifier”. This can be used by users as well as by software in some cases; • An identifier applied to aggregations in the classification scheme hierarchy is called “Classification Code”; • Other Identifiers are named as needed, e.g. “Retention and Disposal Schedule Identifier”.	
3941	The difference between System Identifiers and Classification Codes is illustrated in the following three diagrams. These diagrams are also referred to later in the chapter.	
3940	The first diagram (<7.1>) shows a part of a fictitious, but realistic classification scheme. It shows some of the classes; each class has a class title (as required by <chapter 3 ID2665>).	

ID	Text, Requirement & Rationale	Testable
690	**7 Referencing**	
3939	 Diagram <C7 ID3939>	
3938	Each class is allocated a System Identifier, as shown in diagram <7.2>.	
3937	 Diagram <C7 ID3937>	
3936	Note that the System Identifiers shown here are short and simple, purely for illustration. In reality they are likely to be longer and more complicated in structure. By way of illustration, an example of a System Identifier based on the "Globally Unique Identifier" algorithm is 0c7220e3-5646-44c4-82b0-67832c1efa1c.	
3935	Classes are also allocated a Classification Code. As specified in the requirements below, this can take several forms; one example is shown in diagram <7.3>.	

ID	Text, Requirement & Rationale	Testable
690	**7 Referencing**	
3934	 Diagram <C7 ID 3934>	
3933	Here also, the Classification Codes are shown as relatively simple, for illustration.	
3932	Each class has a Classification Code that can be combined with the Classification Codes of its parent classes to make a "Fully-Qualified Classification Code". So, for example, the Fully-Qualified Classification Code of the class *Disaster Recovery* is 001-001-003. It is constructed as follows: • start with the Classification Code of its highest parent in the hierarchy (001, being the Classification Code of the class *Corporate Direction*); • add the Classification Code of its next parent down in the hierarchy (001, being the Classification Code of the class *Business Continuity*), making 001-001; • repeat the previous step until the nearest parent class is reached (in this simple example, there are no repeats); • add the Classification Code of the class (003), being the Classification Code of the class *Disaster Recovery*), producing the Fully-Qualified Classification Code 001-001-003.	
2269	The expected usage determines the degree of uniqueness required. System Identifiers generally must be unique within one ERMS "instance" or "network node" at a minimum, and network-wide by preference. Fully-Qualified Classification Codes must be unique within a classification scheme, though because they are built up hierarchically the individual Classification Codes may be unique only within one node (e.g. a class or sub-file) of the hierarchy.	
4462	Where uniqueness across a network is required, it is desirable that system identifiers should be based on an acknowledged standard that guarantees global uniqueness (that is, uniqueness across all systems at all times). This is also desirable for standalone, or non-networked, applications, so as to allow for possible future growth and for potential merger or acquisition activities. Several such standards have been proposed, none of which has a dominant position; MoReq2 therefore does not mandate the use of a specific standard for this purpose.	
3942	Section 7.1 below covers requirements concerning Classification Codes. Section 7.2 addresses System Identifiers.	

7.1 Classification Codes

ID	Text, Requirement & Rationale	Testable
3943	**7.1 Classification codes**	
2263	**Requirement**	
2270	Whenever a new occurrence of any of the following is created in the ERMS, the ERMS must associate with it a Classification Code: • class; • file; • sub-file; • volume;	Y
3804	The ERMS must ensure that all Fully-Qualified Classification Codes are unique within a classification scheme hierarchy.	Y
2268	The ERMS must be able to store Classification Codes as metadata elements of the entities to which they refer.	Y
2267	The ERMS should allow the formats of Classification Codes and Fully-Qualified Classification Codes to be specified by an administrative role at configuration time. It should allow the following features of Classification Codes to be defined, for each level of the hierarchy: • numeric, alphabetic or alphanumeric; • presence or absence of leading zeroes; • minimum length (in the case of leading zeroes); • starting value; • increment.	Y
3802	*Fully-Qualified Classification Codes must consist of a concatenation of Classification Codes separated by a separator character.*	
3945	The ERMS should allow the separator characters in Fully-Qualified Classification Codes to be selected from, at a minimum: • " " (space); • "-" (dash); • "/" (forward slash); • "." (dot).	Y
3946	*The example Classification Code described above could therefore be shown as any of the following, depending on the choices made for leading zeroes and separator at configuration time;* • *1 001 003;* • *001-001-003;* • *1/1/3;* • *001.001.3.*	
2266	The ERMS must allow an administrative role to specify, when a new class is created, whether its descendant entities will have Classification Codes generated automatically by the ERMS or provided by the user/an external application. The ERMS must either: • generate each Classification Code automatically and prevent users from inputting it manually, and from subsequently modifying it (for example, a sequential number, as in the example above); or: • allow an authorised user or an external application to provide the Classification Code, but subsequently prevent them from modifying it.	Y

ID	Text, Requirement & Rationale	Testable
3943	**7.1 Classification codes**	
3757	*An example of the first option is if a new class titled "Incident Management" is added under the class "Business Continuity" in the example shown in diagram <C7 ID3934>; in this example, it would be allocated the Classification Code 004, as shown in diagram <C7 ID3947>:*	
3947	 Diagram <C7 ID3947>	
3948	*The second option is appropriate in case management settings.*	
2265	When the ERMS generates a new Classification Code automatically (the first option in <ID2266), it must generate the next sequential number taking into account: • the most recently used Classification Code at that point in the classification scheme, or (for the first at that point) the starting value; • the increment specified, see <ID2267>).	Y
3949	*See diagram <C7 ID3947> for an example.*	
3956	When accepting a Classification Code from a user or from an external application, the ERMS must validate it for uniqueness within its parent.	Y

7.2 System Identifiers

ID	Text, Requirement & Rationale	Testable
3955	**7.2 System Identifiers**	
4463	**Requirement**	

ID	Text, Requirement & Rationale	Testable
3955	**7.2 System Identifiers**	
3954	Whenever a new occurrence of any of the following is created in the ERMS, the ERMS must associate with it a System Identifier: • classification scheme; • class; • file; • sub-file; • volume; • record; • record extract; • retention and disposition schedule; • document.	Y
3953	The ERMS must ensure that all System Identifiers are unique within a classification scheme hierarchy and within the ERMS instance.	N
3952	*Note that this requirement extends across geographical locations where a distributed classification scheme has been implemented and across classification schemes when more than one classification scheme has been implemented.*	
3951	The ERMS must be able to store System Identifiers as metadata elements of the entities to which they refer.	Y
3950	The ERMS should allocate System Identifiers which are globally unique.	N
3957	*Globally unique means that the System Identifiers are allocated using an algorithm that guarantees no other System Identifier can have the same value, regardless of when it is produced or by which ERMS.*	
3963	*This is desirable to allow for re-configurations, such as those caused by corporate re-organisations, acquisitions and mergers etc. If every entity is not allocated a globally unique System Identifier, the probability of difficulties during re-configurations is high.*	
3962	The ERMS should use the UUID algorithm (as specified in ISO/IEC 9834-8 and ITU-T Rec. X.667) to generate globally unique System Identifiers.	P
3961	*This algorithm, which in some implementations is commonly referred to as GUID (Globally Unique ID), can be used to guarantee uniqueness.*	
3960	*Other approaches to the generation of unique identifiers may be used, including the Digital Object Identifier System (DOI®) and the Uniform Resource Name (URN) scheme.*	
3959	The ERMS must not require users to enter or use System Identifiers for any ERMS function.	P
3958	*This requirement is included because globally unique identifiers tend to be long and not "user-friendly". However, it is acceptable for users to be allowed to use System Identifiers if they choose to.*	

8 Searching, Retrieval and Presentation

ID	Text, Requirement & Rationale	Testable
709	**8 Searching, Retrieval and Presentation**	
4648	**Note to reviewers: This draft uses the term "presentation" where the previous version of MoReq used "rendition". The change follows many requests. Some confusion is inevitable given that "rendition" has numerous meanings in English. The present interpretation is final.**	

ID	Text, Requirement & Rationale	Testable
709	**8 Searching, Retrieval and Presentation**	
710	An integral feature of an ERMS is the ability for the user to retrieve files and records. This includes searching for them, whether or not precise details are not known, and presenting them. Presentation is producing a representation on-screen ("displaying") or printing; it may also involve, as necessary, playing audio and/or video (see Glossary).	
711	Accessing files and records, and then viewing them, requires a flexible and broad range of searching, retrieval and presentation functions to meet the demands of different types of user. Although some advanced search features can be thought of as being beyond classical records management functions, the required functionality is described here on the grounds that an ERMS without good retrieval facilities is of limited value.	
712	This chapter lists requirements for searching and retrieval in section 8.1. Requirements associated with presentation are divided into three sections: section 8.2 lists requirements for display, section 8.3 deals with printing, and section 8.4 addresses the presentation of records which cannot be printed.	
714	All of the features and functionality in this chapter must be subject to access controls as described elsewhere in this specification, including security controls. In other words, the ERMS must never present information to any user which that user is not entitled to receive. To avoid complexity, this is assumed and is not repeated in each detailed requirement.	

8.1 Search and Retrieval

ID	Text, Requirement & Rationale	Testable
715	**8.1 Search and Retrieval**	
716	Searching is the process of identification of records or files through user-defined parameters for the purpose of locating, accessing and retrieving records, classes, files, sub-files, volumes and/or their metadata.	
717	The ERMS search and navigation tools are used to locate metadata, records, volumes, sub-files or files. These require a variety of searching techniques to support users ranging from (for example) the sophisticated "research" user to the "casual" and less "computer literate".	
2271	**Requirement**	
2300	No ERMS search or retrieval function must ever reveal to a user any information (metadata or record content) where the access and security controls (sections 4.1 and 10.16 respectively) prevent access by that user.	P
2289	The ERMS must allow users to search for and retrieve: • records; • every level of aggregation of records (class, file, sub-file, volume); and their associated metadata at any level of the classification system.	Y
2286	The ERMS must allow users to specify any combination of metadata elements as search terms.	Y
4157	*The search facility needs to be able to search on any of the metadata elements, for example, Title.*	
3896	The ERMS must allow users to specify whether a search is to find records or a specified level of aggregation of records.	Y
2288	The ERMS search function should appear to users to be the same for all searches specified in requirement <ID2289>.	Y

ID	Text, Requirement & Rationale	Testable
715	**8.1 Search and Retrieval**	
3758	*In other words, users should see the same interface, features and options whether searching for classes, files, sub-files, volumes or records (though details of the presentation of results may vary according to what is being searched).*	Y
2285	The ERMS must allow users to search for the text content of records.	Y
4502	*This includes the text of records that are inherently textual in nature, such as e-mail messages, and (where the ERMS includes OCR functionality) records which have been converted to text by OCR (se <section 6.7 ID4122>)*	
4074	The ERMS must allow the use of searches to locate a class and/or file for the purpose of declaration, as a part of the declaration process.	
4526	*This is an ease of use requirement. It requires that search functionality be readily available to users who are in the process of capturing one or more records; in other words users must not be forced to quit a capture process to initiate a search.*	
2284	The ERMS must allow users to use any combination of metadata elements and/or textual record content as search terms during a search operation.	Y
4158	*For example a search could combine a named author together with a particular text string in the record.*	
2281	The ERMS should provide a search function which operates in an integrated and consistent manner across both record content and metadata.	Y
3897	*This means that the interface and its behaviour should be the same across these kinds of searches.*	
2273	The ERMS must display the total number of items found as a result of the search (the "hit list"), and display (or allow the user to request display of) the number of items in the hit list.	Y
2295	The ERMS should allow users to refine (i.e. narrow) a search without having to re-enter the search criteria.	Y
3763	*A user should for example be able to start with the hit list from a search, and then perform a further search within that list.*	
2283	The ERMS must allow administrative roles to configure and subsequently change the specification of default search metadata elements including: • any element of record, volume, sub-file, file and class metadata, and • optionally, text.	Y
4529	*This refers to the default window that first appears when a search is initiated; it generally contains a set of fields for metadata elements that are commonly used in searches. This set comprises the default elements in the requirement.*	
3787	The ERMS must provide a search function that allows the use of all Boolean operators namely: • AND; • OR; • EXCLUSIVE OR; • NOT; in any valid combination to combine an unlimited number of search terms.	Y
2812	The ERMS must allow users to search for objects by their keyword(s)	Y
2811	During any search involving keywords, the ERMS must allow users to select keywords controlled vocabularies (or lists of permitted terms).	Y
4532	*Noting requirement <ID4074>, this could be during a capture process, or during any other search.*	
2280	The ERMS should incorporate the use of a thesaurus to enable users to search by concept.	Y

ID	Text, Requirement & Rationale	Testable
715	**8.1 Search and Retrieval**	
3792	Where the ERMS incorporates the use of a thesaurus for concept searching, it should be compliant with at least one of the following standards: • ISO 2788; • ISO 5964.	Y
3759	*This will allow retrieval of documents with a broader, narrower, or related term in their content or metadata. For example, a search for "ophthalmic services" might retrieve "health services", "eye test" or "ophthalmology".*	
3789	*The former standard specifies a monolingual thesaurus and the latter a multilingual thesaurus.* (See *<ID2093> and <ID3636>).*	
2817	Where a controlled vocabulary of keywords takes the form of an ISO 2788-compliant or ISO 5964-compliant thesaurus, the ERMS should allow users who are performing a search to use the full features of the thesaurus, such as broader, narrower and related terms and synonyms in a manner that is fully integrated with the ERMS.	Y
2816	*In other words, if a user is searching for a file, the user may enter a term that is not in the scheme's controlled vocabulary, then use the thesaurus features to find the appropriate preferred keyword. An example is if "budgets" is a preferred keyword: in this case, a user might enter "estimates" and then be guided to its broader term "budgets"; or a user might enter "accounting records" and be presented with a list of narrower terms, one of which is "budgets".*	Y
3794	*For ease of use, users must not have to leave the search interface to access the thesaurus to search for related search terms.*	
3898	Where the ERMS incorporates the use of a thesaurus for concept searching, the ERMS must allow an administrative role to maintain the thesaurus.	Y
3899	*Maintenance is needed for the introduction of new terms and terms specific to the business.*	
2815	The ERMS must restrict to authorised administrative roles the ability to change the keywords associated with a file.	Y
2814	*This facility is intended for exceptional circumstances only, such as to correct clerical errors. Changing keywords inappropriately car seriously compromise the accessibility of records, even if recorded in an audit trail, and so should be avoided.*	
2819	Whenever any keyword of any file is changed, the ERMS must require an administrative role to enter the reason for the change.	Y
2825	Whenever any keyword of any file is changed, the ERMS must keep a clear trace of its status prior to the change so that its history can be determined easily.	Y
2279	The ERMS should provide for partial match and "wild card" searching of metadata that allows for forward, backward and embedded expansion.	Y
3760	*For example:* • *the search term "proj*" might retrieve records containing "project" and "projection" and "PROJA";* • *the search term "psycho*s" might retrieve records containing "psychosis", "psychotics" and "psychologists"* • *the search term "*byte" might return "gigabyte" and "terabyte";* • *The search term "organi?ation" might retrieve records containing "organisation" and "organization".*	
2278	The ERMS should provide word proximity searching.	
4533	*A proximity search finds terms separated by no more than a specified number of words, for example:* • *"International" and "Organisation" separated by no more than one word.*	

ID	Text, Requirement & Rationale	Testable
715	**8.1 Search and Retrieval**	
2276	The ERMS must allow users to limit the scope of any search to any file or aggregation specified by the user at the time of the search.	
2275	The ERMS must be able to search for, and retrieve, a complete electronic file, sub-file or volume, and all its contents and contextual metadata, and display a list of all, and only, the entries in the context of that aggregation in a single retrieval process.	
3762	*This is needed when a user wishes to copy or print the entire contents of a file to take to a meeting, or to facilitate temporary working, or for any other reason.*	
2297	The ERMS must behave in an identical manner when dealing with physical or electronic records in searches, save that: • the content of physical records cannot be presented (instead, the ERMS displays its location metadata, see below); • different metadata may be shown for physical and electronic records.	Y
3797	The ERMS must behave in an identical manner when searching regardless of whether the objects being searched for are stored on-line, near-line or off-line, save that: the mechanism and performance for presenting electronic objects may vary.	Y
4534	*This requirement applies only when the ERMS uses near-line and/or off-line storage in addition to online storage.*	
2296	The ERMS should allow users to save and re-use search terms.	Y
3784	The ERMS should allow users to make saved search terms available for use by other users.	Y
3764	The ERMS should allow users to specify time intervals in search requests, e.g. calendar dates or number of days.	Y
2294	The ERMS should allow the use of time intervals specified either as dates (e.g. 24 Dec 2008 - 5 Jan 2009) or in natural language as search terms, e.g. “last week”, “this month”, allowing the use of at least the following words and/or their equivalents in other languages: • last; • this; • next; • week; • month; • quarter; • year; • names of days of the week; • names of months.	Y
2292	The ERMS should allow users or administrative roles to configure display of the search results, including: • the order in which the search results are presented; • the number of hits displayed on the screen per view from the search; • the maximum number of hits for a search; • which metadata elements are displayed in search result lists.	Y
2291	The ERMS should provide implicit or explicit relevance ranking of the search results.	Y
2301	When a hit list contains an “extract” of an electronic record, or a record for which an extract exists, (see section 9.3), the ERMS should relate the two, so that retrieval of one shows the existence of and allows retrieval of the other, subject to access controls, whilst retaining separate metadata for the two items.	Y

ID	Text, Requirement & Rationale	Testable
715	**8.1 Search and Retrieval**	
3800	The ERMS should allow the configuration of a search engine other than the default search engine.	N
3801	*It may be desirable for an organisation to implement a search engine other than that which is supplied with the ERMS for system compatibility or other reasons.*	

8.2 Presentation: Displaying Records

ID	Text, Requirement & Rationale	Testable
779	**8.2 Presentation: Displaying Records**	
780	An ERMS may contain records with different formats. The user requires generic presentation facilities that will accommodate the display of a range of formats.	
2272	The ERMS must be able to present the contents of any electronic item in a hit list, and/or the metadata of any item in a hit list, by a mouse click or keystroke.	Y
2305	*For example:* • *the ERMS should display a list of the records contained in a file;* • *The ERMS should display the content of a record;* • *The ERMS should display the metadata of a volume..*	
3768	*If the ERMS is storing records in a proprietary application format, it may be acceptable for the presentation to be performed by an application outside the ERMS.*	
2304	The ERMS should be able to present records that the search request has retrieved without loading a software application associated with the record.	Y
3769	*This is typically provided by integrating in the ERMS a viewer software package. This is frequently desirable to increase speed of presentation.*	
2303	The ERMS should be able to present all the types of electronic records specified by the organisation in a manner that preserves the information of the records (e.g. all the features of visual presentation and layout produced by the generating application package), and which presents all components of an electronic record together.	N
3770	*The organisation needs to specify the application packages and formats required, and in some cases acceptable levels of fidelity. In many cases (e.g. in typical office environments) the fidelity need not be specified in detail; however rigorous specification of fidelity may be need for applications which rely on detailed interpretations, such as records including high-resolution X-ray images.*	

8.3 Presentation: Printing

ID	Text, Requirement & Rationale	Testable
790	**8.3 Presentation: Printing**	
791	This section applies only to records and other information whose content can be printed in a way that is understandable. It does not apply to, for example, audio or video files.	
792	The ERMS must provide printing facilities, to allow all users to obtain printed copies of printable records, their metadata, and of other administrative information.	
3901	In all requirements, "printing" is understood to include features normally associated with report production, such as multi-page reports, page numbering, dated headings, and the use of any configured printer. Sending screen image dumps to a printer is not normally considered sufficient for these requirements.	
2306	**Requirement**	

ID	Text, Requirement & Rationale	Testable
790	**8.3 Presentation: Printing**	
2319	The ERMS must be able to print the content of records and specified elements of their metadata.	Y
2318	The ERMS must allow the printing of all or specified metadata for any class, file, sub-file, volume or record.	Y
2317	The ERMS must allow all records in a class, file, sub-file or volume to be printed in one operation.	Y
2316	The ERMS must allow users to specify a subset of metadata elements (such as Title, Author, Creation date) and print out a summary list of these elements for selected aggregations of records.	Y
2315	The ERMS should allow an administrative role to specify at configuration time that all printouts of records contents have selected metadata elements appended to them (e.g. title, registration number, date, security category) by default.	Y
4535	*This could be used, for example, to ensure that whenever a record is printed, its security category is printed at the same time, as a security measure.*	
4160	The ERMS should allow users, at the time of printing, to amend the default metadata elements that are appended to printouts.	Y
2314	ERMS must allow users to print hit lists (see section 8.1) resulting from a search.	Y
2313	The ERMS must allow an administrative role to print all or a selection of administrative parameters.	Y
4161	*For example a list of all users with a specific security category.*	
2312	The ERMS must allow an administrative role to print retention and disposition schedules.	Y
2311	If a thesaurus is integrated (see <ID2280>) the ERMS should allow administrative roles to print the thesaurus.	Y
2824	The ERMS must be able to print out a list of each controlled vocabulary (a list of all permitted terms).	Y
2823	*It is acceptable to print the list from thesaurus management software where this is integrated with the ERMS.*	
4536	The ERMS should be able to export a list of each controlled vocabulary (a list of all permitted terms).	Y
2822	Where a controlled vocabulary of keywords takes the form of an ISO 2788-compliant or ISO 5964-compliant thesaurus, the ERMS should be able to print out the thesaurus entries, showing all terms and their relationships.	Y
4537	*Printing of ISO standards-based thesauri should be compatible with the representational guidelines given in ISO 2788 and ISO 5964.*	
2821	*It is acceptable to print this from separate thesaurus management software that is integrated with the ERMS.*	
2310	The ERMS must allow authorised roles to print all or part of the classification scheme.	Y
2309	The ERMS must allow administrative roles to print all or part of the file repertory (if used; see <C3 ID2091>).	Y
2308	The ERMS must allow administrative roles to print all or part of audit trails (see <IDxxxx>).	Y
2307	The ERMS must be able to print the formats specified by the organisation. Printing must: • preserve the layout produced by the generating application package(s); • include all printable components of the electronic record.	Y
3771	*The organisation needs to specify the formats required.*	

8.4 Presentation: Other

ID	Text, Requirement & Rationale	Testable
822	**8.4 Presentation: Other**	
823	This section applies only to records and other information whose content cannot be printed in a way that is understandable, such as audio or video files.	
2320	**Requirement**	
2321	The ERMS must include features for presenting and outputting to appropriate media records which cannot be printed.	P
3772	*Examples include audio, video, and some web-sites. The organisation will need to specify the nature of these records.*	

9 Administrative Functions

ID	Text, Requirement & Rationale	Testable
829	**9 Administrative Functions**	
830	This section covers the maintenance and system support functionality required by an ERMS. These facilities allow administrative roles to manage change in the user population and parameters affecting the behaviour of the system.	
3902	This functionality must provide administrative roles with the ability to manage events such as maintaining the user base and, crucially, the permissions assigned to users. The system must also provide monitoring capability for system errors.	
831	Some of these facilities may be provided by an associated EDMS, database management system, operating system, or by other applications.	
832	Requirements are listed in this chapter for: • general administration (section 9.1); • system reporting (section 9.2); and for • changing, deletion and redaction of records (section 9.3).	
3905	Closely-related features are described in chapter 4, namely; • Access permissions in section 4.1; • backup and restore in section 4.3.	

9.1 General Administration

ID	Text, Requirement & Rationale	Testable
833	**9.1 General Administration**	
834	This section includes requirements for managing system parameters, system management and configuration, and user administration.	
4538	In large organisations, the functionality described in this section may be assigned to an operations function rather than to an application administrator. However, in small organisations, they may be assigned to an administrator.	
2322	**Requirement**	
2330	The ERMS must allow administrative roles, to retrieve, display and re-configure systems parameters and settings made at configuration time.	Y
3903	*These settings include, for example, configuration of access rights.*	
3904	The ERMS must allow administrative roles to • allocate functions to users and roles; • allocate one or more users to any role.	Y

ID	Text, Requirement & Rationale	Testable
833	**9.1 General Administration**	
2327	The ERMS must monitor available storage space, and notify administrative roles when action is needed because available storage is below a level set at configuration time, or because of another error condition.	Y
4178	*It is acceptable for administrative roles to be notified by means of separate system management software.*	
2326	Where the storage supports error rate reporting, the ERMS should monitor error rates occurring on storage media, and report to administrative roles any medium or device on which the error rate is exceeding a parameter set at configuration time or at a later date.	N
3775	*This applies particularly to optical media.*	
4179	*It is acceptable for administrative roles to be notified by means of separate system management software.*	
2325	The ERMS must allow administrative roles to make bulk changes to the classification scheme, ensuring all metadata and audit trail data are handled correctly and completely at all times, in order (for example) to support restructuring within the organisation. These changes must include, but need not be limited to: • the division of a class into two (i.e. dividing a class into two new classes, at the same level, including moving all the descendant classes and the information allocated to them); • the combination of two classes into one (i.e. moving a class into another existing class, including moving all its descendant classes and the information allocated to them); • the movement of a class (including all descendant classes and the information allocated to them); • the re-naming of a class; • changing access permissions to a class (and its descendant classes and therefore all information allocated to them); • changing the retention and disposal schedule allocated to a class (and its descendant classes and therefore all information allocated to them), following the same logic for inheritance and conflicts as in section 5.1 (especially requirements <ID2988> and <ID2183>.	Y
4010	*When a classification scheme is designed along functional lines, most of these functions are unlikely to be needed. However, they will be needed when a classification scheme, or a part of it, is designed to match an organisational structure.*	
3906	When a bulk change is made: • closed files must remain closed, retaining their references to the classification scheme before the change; open files must either: • be closed, retaining their references to the classification scheme before the change, and cross-referenced to a new file in the changed scheme in metadata; • be referenced to the changed scheme, but clearly retaining all prior references to the classification scheme before the change in metadata.	Y
3907	*The term "bulk changes" implies that all classes, files, sub-files, volumes and records affected can be processed with a single transaction, rather than needing to be processed individually.*	
2324	The ERMS should allow administrative roles easily to move users between organisational units.	Y
4539	*In particular, it should be possible to move a user without having to delete the user from the ERMS and re-enter the user's details.*	

9.2 Reporting

ID	Text, Requirement & Rationale	Testable
854	**9.2 Reporting**	
4012	Flexible reporting is an important feature in an ERMS. It is required so that administrative roles can manage the system; and so that management can monitor it to ensure it is used appropriately.	
3908	An ERMS needs to be able to provide a number of management, statistical and ad hoc reports so that administrative roles can monitor system activity and status. This reporting is required across the entire system, including: • the classification scheme; • files and records; • user activity; • access and security permissions; • disposition activity.	
3909	The ERMS must provide a number of standard reports capable of being configured by administrative roles and should be flexible to enable ad hoc reports to be produced on demand.	
855	Ideally the ERMS will include a report-writing sub-system, with all the flexibility and features that implies. However, it is not appropriate to attempt to reproduce here the requirements for a comprehensive report writing sub-system, so this section gives outline requirements only. In any implementation, the amount and complexity of reporting will be determined by organisational features including the size, complexity and levels of change to the classification scheme, the amount and nature of the records, and the user base.	
2331	**Requirement**	
2333	The ERMS must allow administrative roles to produce periodic reports (daily, weekly, monthly, quarterly) and to specify ad hoc reports.	Y
3917	The ERMS must include features for printing reports, viewing them on-screen and storing them in electronic form online.	Y
4013	*As in section 8.3, "printing" is understood to include features normally associated with report production such as multi-page reports, page numbering, dated headings, configurable page headers and footers, and use of any configured printer). Sending screen image dumps to a printer is not normally considered sufficient for these requirements.*	
3921	*For example, users may wish to work with the contents of a report using spreadsheet software. MoReq2 does not specify the format(s) to be used for such exports.*	
4014	The ERMS should allow time periods covered by a report to be configured either as a date range (e.g. 24/12/2008 - 5/1/2008) or as a time interval specified in natural language (as in <chapter 8 ID2294>).	Y
2335	The ERMS must include features for sorting and selecting the information included in reports.	Y
4015	*For example, users should be able to specify which columns of a columnar report are used to sort the report contents.*	
2334	The ERMS should include features for totalling and summarising report information.	Y
4016	The ERMS should include features for graphical reporting.	Y
4017	*For example, trend-reports showing changes in reported information over time, or histograms.*	
3919	The ERMS must enable report requests to be saved for future re-use.	Y
3920	The ERMS must enable reports to be exported for use in other applications.	Y

ID	Text, Requirement & Rationale	Testable
854	**9.2 Reporting**	
3911	The ERMS must be able to provide reports on the total number and location of: • files, sub-files and volumes; • records, sorted by file format and version; • files, sub-files and volumes, sorted by access control and security markings; • electronic files, sub-files and volumes, sorted by size; • electronic files, sub-files and volumes, sorted by storage location; • vital records.	Y
3912	The ERMS must be able to provide reports on: • the rate of capture of records; • rate of retrieval of records; • rate of creation of new classes and files.	Y
4018	The ERMS should allow the reports described in <ID3912> to be for any combination of: • across the entire system or for specified classes; • specified user groups or users; • a specified range of dates.	Y
2138	The ERMS should be able to provide reports for actions on files and records organised by user, by workstation and (where technically appropriate) by network address.	Y
4019	The ERMS should allow the reports described in <ID3912> to cover a specified time interval within several days.	Y
4020	*For example, showing hourly figures, to allow peaks and troughs of activity to be monitored.*	
2336	The ERMS must be able to produce a report listing files, sub-files and volumes, for all or part of the classification scheme, structured to reflect the classification scheme.	Y
3910	The ERMS must be able to provide a report on the amount of system storage space currently in use and available.	Y
2338	The ERMS must allow administrative roles to produce reports on the audit trail. These reports must include, at a minimum, reporting based on any selected: • class; • file; • sub-file; • volume; • record; • user; • time period.	Y
2337	The ERMS should allow administrative roles to enquire on and produce audit trail reports based on selected: • security categories; • user groups; • other metadata.	Y
3915	The ERMS must be able to report on the outcome of a disposal process listing the classes, files, sub-files, volumes and records successfully disposed of and any failures.	Y
3916	The ERMS must be able to provide reports on the outcome of an export process listing the classes, files, sub-files, volumes and records successfully exported and any failures.	Y
3924	The ERMS must be able to provide administrative roles with reports on disposition activity, including disposition actions that are overdue.	Y
2332	The ERMS should allow administrative roles to restrict users' access to selected reports.	Y

ID	Text, Requirement & Rationale	Testable
854	**9.2 Reporting**	
3923	The ERMS must be able to provide administrative roles with a report on attempted access control and other security policy violations.	Y
4021	*This requirement only applies when the ERMS (and/or the operating system) is configured so as to allow an item's existence to be visible to a user even though the user is not allowed access to it. It is not relevant when the ERMS is configured to hide the existence of an item which cannot be accessed.*	
2210	Administrative roles should be able to specify the frequency of a retention and disposition schedule reporting, the information reported and highlighting exceptions such as disposition overdue.	Y
2962	The ERMS should provide quantitative reports on the volumes and types of records to be reviewed within a specified period.	Y
2204	The ERMS should support reporting and analysis tools for the management of retention and retention schedules by an administrative role, including the ability to: • list all retention schedules; • list all electronic files to which a specified retention schedule is assigned; • list the retention schedule(s) applied to all files in a class; • identify, compare and review retention schedules (including their contents) across the classification scheme; • identify formal contradictions in retention schedules across the classification scheme.	Y
2212	The ERMS should be able to accumulate statistics of review decisions in a given period and provide tabular and graphical reports on the activity.	Y
2225	The ERMS must produce a report detailing any failure during a transfer, export or deletion. The report must identify any records destined for transfer which have generated processing errors, and any files or records which are not successfully transferred, exported or deleted.	Y
2220	The ERMS should provide the ability to sort electronic files selected for transfer into ordered lists according to user-selected metadata elements.	Y
2219	The ERMS should provide the ability to generate user-defined forms to describe electronic files that are being exported or transferred.	Y

9.3 Changing, Deleting and Redacting Records

ID	Text, Requirement & Rationale	Testable
884	**9.3 Changing, Deleting and Redacting Records**	
885	A basic principle of recordkeeping is that records cannot normally be changed, and (except at the end of their life cycle in the ERMS) files, sub-files, volumes and records cannot normally be destroyed.	
3926	This section deals with the requirements for exceptional situations where the content of a declared record may need to be amended, or a record deleted and replaced.	
886	Administrative roles may need to "delete" records to correct errors to meet legal requirements, for example, under data protection legislation.	
3927	The action of deletion may mean one of two things: • destruction (see <ID2231> and <ID2217>); • retention, accompanied by a notation in the record's metadata that the record is considered removed from records management control.	

ID	Text, Requirement & Rationale	Testable
884	**9.3 Changing, Deleting and Redacting Records**	
889	In either case, deletion is to be exceptional, and so the ability to delete must be tightly controlled in order to protect the general integrity of the records. In particular, information about deletions must be stored in the audit trail.	
4022	*If local legislation or regulation imposes different requirements, for example relating to the expunging of personal data, this should be addressed in a national chapter zero.*	
890	Administrative roles sometimes need to publish, or make available, records containing information which is still sensitive, without revealing the sensitive information. This can result from data protection rules, security considerations, commercial risk, etc. For this reason, administrative roles need to be able to mask the sensitive information, without affecting the underlying record.	
3928	The process is referred to here as redaction. When the process of redaction is carried out, the result is the original record (unchanged), and a copy of the record which has been masked in some way (the redacted copy, or "extract" of the original record). The ERMS stores both the original record and the extract.	
4023	In principle, redaction can apply to any kind of record - text, image, audio, video etc.	
891	Note that deletion and change are also discussed in chapter 5.	
2340	**Requirement**	
2354	The ERMS must allow a configuration option, as an alternative to <ID2353 below>, which prevents any record, once captured, from being, deleted or moved by any administrative or user role; see also <ID below>.	Y
3777	*This requirement does not affect transfer or destruction of records in accordance with a retention and disposition schedule, as described in section* 5.3. *It is intended for environments in which the deletion of records (as described above) is either unnecessary or not permitted.*	
2353	The ERMS should allow a configuration option, as an alternative to <ID2354 above>, that "deletion" of a record is implemented as destruction of that record, and that relocation of a record results in moving the record.	Y
4540	*This is not regarded as good practice in records management. It is included here only for situations in which it is considered unavoidable. In most situations, the option specified in <ID2354 above> should be preferred.*	
4595	If the option in <ID2354 above> is selected, the ERMS must behave as follows: • If an administrative role "deletes" a record (as in <ID2348>) the record's metadata must be marked accordingly, and the ERMS must hide the content and metadata of the record from all users save for suitably-authorised administrative roles, as if it were deleted. • If an administrative role "re-locates" a record (as in <ID2123>), exactly the same behaviour as for a deletion but with the addition that a copy must be inserted automatically at the new location.	Y
3929	If the option in <ID2353 above> is selected, the ERMS must behave as follows: • If an administrative role "deletes" a record (as in <ID2348>) the record's metadata must be marked accordingly, and the ERMS must hide the content and metadata of the record from all users save for suitably-authorised administrative users, as if it were deleted. • If an administrative role "re-locates" a record (as in <ID2123>) exactly the same behaviour as for a deletion but with the addition that a copy must be inserted automatically at the new location.	Y

ID	Text, Requirement & Rationale	Testable
884	**9.3 Changing, Deleting and Redacting Records**	
2350	Subject to support for <ID Security metadata element> and <ID2178>, an administrative role must be able to change the security category of classes, files, sub-files, volumes and records.	Y
2351	An administrative role must be able to change the security category of all records in a class, file, sub-file or volume in one operation.	Y
3779	*This is routinely required to reduce the level of protection given to records as their sensitivity decreases over time.*	
4177	The ERMS must provide a warning to an administrative role if any records are having their security category lowered, and await confirmation before completing the operation.	Y
2349	The ERMS must record the full history, i.e. dates and details of any changes to security category, in the metadata of the relevant class, file, sub-file, volume or record.	Y
2348	Subject to <ID 2354 above>, the ERMS must allow administrative roles to delete classes, files, sub-files, volumes and records outside the disposition process.	Y
3780	*This is intended for use only in the event of the exceptional circumstances described in this section.*	
3930	In the event of any deletion as defined above, the ERMS must: • record the deletion in the audit trail; • produce a report for administrative roles; • delete the entire contents of a class, file, sub-file or volume when it is deleted; • ensure that no documents are deleted if their deletion would result in a change to another record (for example if a document forms a part of two records - see <ID2884> - one of which is being deleted); • highlight to administrative roles any links from another file, or record to a file, sub-file or volume which is about to be deleted, requesting confirmation before completing the deletion; • maintain complete integrity of the metadata at all times.	Y
2347	Administrative roles must be able to change any user-entered metadata element.	Y
3781	*This functionality is intended to allow administrative roles to correct user errors such as data input errors, and to maintain user and group accesses. Good practice generally will require that users correct their errors whenever possible; this requirement does not prevent users from doing so.*	
3968	Information about all changes to all metadata elements must be stored in the audit trail	Y
2346	The ERMS must allow administrative roles to create one or more extract(s) of a record, for the purposes of redaction, while retaining the original record.	Y
3782	*It may be necessary, in some cases, to provide extracts for several parties in which different parts of the record have been redacted.*	
2345	The ERMS must provide a solution for removing or hiding sensitive information within the extract for all record formats required by the organisation.	P
3970	*If the ERMS does not provide these facilities, it must allow for other software packages to integrate with it and do so. It is acceptable for the ERMS to render a record to a different file format to permit the redaction of a copy, provided that the rendition maintains sufficient fidelity.*	
3783	*It is essential that when the features in <ID3969 above> and <ID4345 above> or any other redaction features are used, none of the removed or hidden information can ever be retrieved from the extract, whether on screen, when printed, played back or in any other form of presentation. This is regardless of the use of any presentation features such as rotation, zooming or any other manipulation including opening the extract in a different software package.*	

ID	Text, Requirement & Rationale	Testable
884	**9.3 Changing, Deleting and Redacting Records**	
2344	When an extract is created, the ERMS must be able to record, either automatically or by manual input, its creation in the record's metadata, including date, time, creator and reason for creation.	Y
2343	Upon creation of an extract the ERMS should automatically declare extracts as records, classifying them in the same file as the original record and prompting the creator of the extract for: • a reason; • security category (where applicable); • optionally, a file into which a copy of the extract will be declared.	Y
3972	Upon creation of an extract the ERMS should allow the copying of metadata elements to the extract.	Y
3973	Subject to access control rights the ERMS should enable amendment of selected data items, for example, security category metadata.	Y
2342	The ERMS should store a cross reference (as in <Metadata ID>) to an extract in the same class, file, sub-file or volume as the original record, even if that class, file, sub-file or volume is closed.	Y
4544	*This is in addition to the requirement to file a copy, in <ID2343>, to allow for cross referencing even in the same file, as the original and extract may be separated by large numbers of records in the file.*	
3971	When a record is retrieved the ERMS must show, or allow the user to see, the existence of all extracts made from that record and, subject to access and security controls, make them available for retrieval.	Y
4024	When an extract is retrieved the ERMS must show, or allow the user to see, the existence of the original record and, subject to access and security controls, make it available for retrieval.	Y
2341	The ERMS must store in the audit trail any change made as a result of any requirement in this section.	Y

10 Optional Modules

ID	Text, Requirement & Rationale	Testable
923	**10 Optional Modules**	
924	This chapter contains requirements functionality closely allied to electronic records management. It covers requirements to support the management of physical (non-electronic) records, document management, workflow, electronic signatures and other functionality.	
3549	Each of the sections in this chapter corresponds to one optional module of the MoReq2 Testing Framework. These modules are optional in the sense that the requirements therein do not form a mandatory part of the core functionality of a MoReq2 compliant ERMS.	
3550	The requirements in this chapter are for functionality which may be integrated with an ERMS. These optional requirements need to be taken together with the core requirements in the rest of MoReq2. Their applicability will depend on whether the organisation has a need to implement the optional functionality.	

ID	Text, Requirement & Rationale	Testable
923	**10 Optional Modules**	
3442	Compliance with the requirements in this chapter is not required for MoReq2 compliance. Therefore mandatory requirements in this chapter are mandatory only in the context of the optional modules in which they are located – that is, they are mandatory only when the optional module in which they are located is included in a test.	
926	In each case, requirements are presented at a high level. As they do not define the core functions of an ERMS, these requirements are not exhaustive but rather provide an indication of the appropriate activities.	
927	The sections in this chapter list requirements for the following areas: • not used – retained in this draft for numbering purposes only (section 10.1); • management of physical records (section 10.2); • disposition of physical records (section 10.3); • document management and collaborative working (section 10.4); • workflow (section 10.5); • casework (section 10.6); • integration with content systems (section 10.7); • electronic signatures (section 10.8); • encryption (section 10.9); • digital rights management (section 10.10); • interoperability and openness (section 10.11); • distributed systems (section 10.12); • offline and remote working (section 10.13); • fax integration (section 10.14); • security categories (section 10.15).	

10.1 Non-hierarchical Classification Schemes

Note to reviewers: following careful consideration by the MoReq2 Editorial Board and consultation with the MoReq2 Vendor Panel this section has been deleted. MoReq2 will not contain requirements for non-hierarchical Classification Schemes. This heading is retained in this draft for numbering purposes only.

10.2 Management of Physical (Non-electronic) Files and Records

Note to reviewers: following careful consideration by the MoReq2 Editorial Board and consultation with the MoReq2 Vendor Panel the concept of hybrid files has been removed from MoReq2. Refer to the revised entity-relationship model for details.

ID	Text, Requirement & Rationale	Testable
936	**10.2 Management of Physical (Non-electronic) Files and Records**	
937	In addition to the electronic records, an organisation's records repository may contain non-electronic records. These can include paper-based records and records on other analogue media, for example microfiche or audio tapes. They may also include digital records stored on portable media, such as CDs, DVDs and computer tapes.	

ID	Text, Requirement & Rationale	Testable
936	**10.2 Management of Physical (Non-electronic) Files and Records**	
4165	The term physical records is used in MoReq2 to mean any record that is held in a medium outside the ERMS. This includes not only analogue media but also digital media holding records that are not individually controlled by the ERMS. For example: • a CD-ROM containing 10,000 images which are not individually recognised by the ERMS as records is a physical record; • a CD-ROM containing 10,000 images, and located in a drive or jukebox connected to the ERMS, and with each of the images recognised by the ERMS as a record is not a physical record – it is a removable medium on which electronic records are stored.	
925	This specification does not address the business need to manage and maintain physical records. Such a need may or may not exist, according to the legislative and regulatory environment. Where it does exist, care needs to be taken to preserve the integrity and accessibility of electronic and physical records taken as a whole. These issues should be addressed by appropriate organisational policies.	
3338	The ERMS must be able to accommodate references to these physical records as well as, and together with electronic records; and provide for the management of aggregations made up of both electronic and physical records. Classes, files, sub-files and volumes may all contain any combination of electronic records and physical records. This differs from the entity-relationship model in the previous version of MoReq.	
3561	Physical records can co-exist with electronic records in several scenarios. The scenarios include: • A file, sub-file or volume contains only physical records. In this case, the entity represented in the ERMS represents a physical container for the records, such as a filing jacket; • A file, sub-file or volume contains both electronic and physical records. The physical records are stored without a container relevant to records management – for example, an engineering drawing stored along with unrelated drawings in a drawing cabinet.	
3562	The ERMS must provide features to allow physical containers (as in the first option) to be managed.	
3565	In order to manage physical records the ERMS must be able to capture and manage metadata about them. This metadata enables administrative and user roles to locate, track, retrieve, review and dispose of physical records, and to allocate access controls to them in the same way as to electronic records.	
3566	Similarly, the ERMS must be able to capture and manage metadata about physical containers.	
2355	**Requirement**	
3569	The ERMS must allow an administrative role to identify classes, files, sub-files and volumes that exist as a physical container.	Y
4479	The ERMS must allow administrative and user roles to enter and maintain metadata about classes, files, sub-files and volumes that exist as physical containers, as specified in the MoReq2 metadata model.	Y
3570	The ERMS must allow user roles to enter and maintain information about physical records in classes, files, sub-files and volumes, following the same rules as when declaring electronic records.	Y
2363	The ERMS must allow classes, files, sub-files and volumes to contain electronic records and physical records together, in any combination.	Y
3326	The ERMS must allow physical records to be managed in the same way as the electronic records, including any inheritance of metadata.	P

ID	Text, Requirement & Rationale	Testable
936	**10.2 Management of Physical (Non-electronic) Files and Records**	
3327	When a user is browsing, retrieving, or otherwise working with a class, file, sub-file or volume, the ERMS should indicate the presence of any physical file, sub-file, volume or records in it with appropriate indicators.	Y
3577	*A user needs to determine easily whether physical entities exist in order to ensure that all records are managed in the same manner. MoReq2 does not prescribe the nature of these indicators.*	
2361	The ERMS must allow a different set of metadata elements to be configured by an administrative role for physical classes, files, sub-files, volumes and records than for the electronic equivalents. As an example, physical file metadata must include (but not be limited to) additional metadata for: • information on its physical location (see chapter 12 <ID2586>); • information regarding the format of the physical file.	Y
2359	The ERMS must ensure that retrieval of any class, file, sub-file or volume simultaneously retrieves the metadata for both electronic and physical entities associated with it in a single operation.	Y
2360	The ERMS should support tracking of physical files, sub-files or volumes by the provision of check-out and check-in to record their location, custodian and the date of check-in/check-out.	Y
2357	The ERMS must ensure that the metadata for physical files, sub-files, volumes and records is always subject to the same access controls as would be the case if they were purely electronic.	Y
2161	The ERMS should provide a tracking function to allow users to record information about the location and movement of physical files, sub-files and volumes.	Y
4480	The ERMS tracking function should allow for locations of physical entities to be selected from or validated against a list (such as a pull-down list).	Y
4481	*Where the ERMS does not support a list of locations, non-validated free text is acceptable.*	
4482	The ERMS tracking function must allow users to enter the checking out and checking in of physical entities.	Y
4483	*In other words, the ERMS must provide facilities to record whether a physical entity is in its home location or has been checked out.*	
2160	The ERMS tracking function must record information about movements which includes: • unique identifier; • current location; • an administrator-defined number of previous locations (the number to be defined at configuration time); • date moved from location; • date received at location; • user responsible for the move (where appropriate).	Y
3329	The ERMS must allow a user role to see the current location of a checked-out physical entity, its custodian, and the date upon which the check out occurred, subject to access control rights.	Y
3330	The ERMS must record all check in and check out activities and dates within the audit trail.	Y
2371	The ERMS must be able to record in the audit trail all changes made to the metadata values of physical entities.	Y
3336	*For example the location metadata element.*	

ID	Text, Requirement & Rationale	Testable
936	**10.2 Management of Physical (Non-electronic) Files and Records**	
2356	The ERMS should support the printing and recognition of bar codes for files, sub-files volumes and records; or alternative tracking systems such as Radio Frequency Identification (RFID) technology.	Y
3333	*This enables the ERMS to track the location and movements of physical records.*	
3578	The ERMS should support the printing of labels for physical files, sub-files and volumes.	Y
3579	*This enables a label to be produced containing essential metadata which can then be attached to the physical entity. This could include, but is not limited to, such metadata as:* • *Title;* • *Identifier - System;* • *Classification Code;* • *Date of Opening;* • *Security Category (if used);* • *Normal storage location.*	
4467	The ERMS should be able to notify administrative roles of any events in the Retention and Disposition Schedule relating to non-electronic records and aggregations scheduled since a restore was executed.	Y
4468	*Chapter 4.3 Backup and Recovery sets out the requirements for restoring an ERMS. When the system is used for managing non-electronic records a disparity may arise following a restore whereby disposition actions have been carried out on the physical objects, but this is not shown in the ERMS. This requirement enables administrative roles to apply remedial action.*	

10.3 Disposition of Physical Records

Note to reviewers: following careful consideration by the MoReq2 Editorial Board and consultation with the MoReq2 Vendor Panel, the concepts of physical and hybrid files, sub-files etc. have been removed from MoReq2.

ID	Text, Requirement & Rationale	Testable
959	**10.3 Disposition of Physical Records**	
2366	**Requirement**	
3964	When the retention period for a retention and disposition schedule ends, if that retention and disposition schedule applies to any physical files, sub-files, volumes or records the ERMS must notify an administrative role.	Y
2372	The ERMS must alert an administrative role to the existence and location of any physical file, sub-file, volume or record associated with any class, file, sub-file volume or record that is to be transferred, exported or destroyed.	Y
4485	*This may be either when the retention period for a retention and disposition schedule ends, or when a transfer or export is initiated.*	
2369	Whenever any physical entities are exported or transferred, the ERMS must export or transfer the metadata for them in the same way as the metadata for the electronic entities.	Y
2222	On transfer, export or destruction of physical entities the ERMS must require an administrative role to confirm the physical transfer, export or destruction before the transfer, export or destruction is completed.	Y
3444	*This normally will require an administrative role to enter manually a confirmation that the physical records have been transferred or destroyed.*	

10.4 Document Management and Collaborative Working

<table>
<tr><th>ID</th><th>Text, Requirement & Rationale</th><th>Testable</th></tr>
<tr><td>981</td><td>10.4 Document Management and Collaborative Working</td><td></td></tr>
<tr><td>982</td><td>Electronic Document Management Systems - EDMSs - are widely used in organisations to provide management and control over electronic documents. Many EDMS functions and facilities overlap with ERMS. EDMSs typically include indexing of documents, storage management, version control, close integration with desktop applications and retrieval tools to access the documents. Some ERMSs provide full EDMS capability, others a subset. Conversely some EDMSs have incorporated core record management functions.</td><td></td></tr>
<tr><td>3414</td><td>EDMSs often form part of a wider system implementation and contain collaborative working tools to enable a number of users to participate in document drafting.</td><td></td></tr>
<tr><td>3647</td><td>Collaborative working is also an integral element of content management systems. See chapter 10.7 for further requirements regarding these features.</td><td></td></tr>
<tr><td>983</td><td>By way of clarification, the following table shows typical differentiators between an EDMS and an ERMS.</td><td></td></tr>
<tr><td>3410</td><td>
<table>
<tr><th>An EDMS…</th><th>An ERMS…</th></tr>
<tr><td>• allows documents to be modified;</td><td>• prevents records from being modified;</td></tr>
<tr><td>• allows documents to exist in several versions;</td><td>• allows a single final version of a record to exist;</td></tr>
<tr><td>• may allow documents to be deleted by their owners;</td><td>• prevents records from being deleted except in certain strictly controlled circumstances;</td></tr>
<tr><td>• may include some retention controls;</td><td>• must include rigorous retention controls;</td></tr>
<tr><td>• may include a document storage structure, which may be under the control of users;</td><td>• must include a rigorous record arrangement structure (the classification scheme) which is maintained by an administrative role;</td></tr>
<tr><td>• is intended primarily to support day-to-day use of documents for ongoing business.</td><td>• may support day-to-day working, but is primarily intended to provide a secure repository for business records.</td></tr>
</table>
</td><td></td></tr>
<tr><td>1003</td><td>The rest of this section sets out key requirements to be considered in provision of an integrated ERMS/EDMS solution. The requirements apply only where EDMS facilities are part of the ERMS. A central feature of these requirements is the concept that documents can be stored in (that is, classified to) the same classes and files as records, though this is optional. This supports the idea that draft documents can be filed in the same files as the final versions, which will be records.</td><td></td></tr>
<tr><td>3581</td><td>Note that the word ‘document’ is used here specifically to describe information or an object that has not been declared as a record in the ERMS.</td><td></td></tr>
<tr><td>2376</td><td>Requirement</td><td></td></tr>
<tr><td>2382</td><td>The ERMS should be able to manage electronic documents and records in the context of the same classification scheme, using the same access control mechanisms.</td><td>Y</td></tr>
<tr><td>4566</td><td>The intention of this requirement is to allow users to store documents that are drafts in the files that the eventual record will be classified to. This is optional.</td><td></td></tr>
</table>

ID	Text, Requirement & Rationale	Testable
981	**10.4 Document Management and Collaborative Working**	
3421	Where the ERMS manages both documents and records within the same classification scheme it must clearly indicate which items are documents and which are records.	Y
3590	*MoReq2 does not specify how this is achieved.*	
3424	Where the ERMS manages both documents and records within the same classification scheme it must allow user roles to perform the following tasks for any specified class or file: • declare all documents as records; • delete all documents, leaving only the records; • delete all documents that are older than a specified age.	Y
3423	Where the ERMS manages both documents and records within the same classification scheme it must notify an administrative role if documents exist within a class or file being exported and provide options to: • enable the documents to be deleted; • declare them as records; • export them with the records.	Y
2388	Where an EDMS is part of an ERMS, or is tightly integrated with an ERMS, the EDMS must be able to capture automatically electronic documents arising in the course of business and pass electronic documents automatically to the ERMS.	P
2387	The ERMS must allow users to: • capture an electronic document and declare it as a record in one process; or • capture an electronic document, store it, and complete the capture by declaring it as a record at a later time.	Y
2377	The ERMS must be able to copy the contents of an electronic record, in order to create a new and separate electronic document without automatically creating a new record, while ensuring retention of the original record intact.	Y
3325	*For example, a user may copy a record in order to send a copy to a recipient who is not a user of the ERMS. This copy may or may not be declared as a fresh record according to the context.*	
3582	The ERMS must allow user roles to check out (see <ID3584 below> any document to which they have appropriate access rights.	Y
4549	The ERMS must allow user roles to check in any document that they have checked out, giving the user the option of checking it in as a new version or not (see <ID3595 below>).	Y
3597	The ERMS should allow a user who checks in a document to enter, optionally, a textual explanation of the changes made while it was checked out.	Y
3584	When a document is checked out by a user, the ERMS must prevent any other user from checking it out or changing it (subject to <ID4630>).	Y
3583	*When a document is checked out, only the user who has checked it out can edit it.*	
3585	*This applies to documents only. As a matter of definition, the ERMS must not allow any record to be checked out and amended.*	
3586	When a document is checked out, if any other user attempts to check it out, the ERMS must prevent the user from checking it out a second time, must inform the user that it is checked out, and must either: • show the identity of the user who performed the checkout; or • conceal the identity of the user who performed the checkout; the option being specified at configuration time.	Y

ID	Text, Requirement & Rationale	Testable
981	**10.4 Document Management and Collaborative Working**	
4630	The ERMS must allow an administrative role to cancel the check out of a document.	Y
4631	*This is intended to allow for situations where the user who checked out the document is unable to check it back in. This situation can arise for several reasons, for example:* • *the user checked it out to a PC that has failed or has been stolen;* • *the checked out document has become corrupted;* • *the user has forgotten to check it back in before starting a period of leave.*	
4632	A user must not be able to check in a version of a document that has had its check out cancelled (as in <ID4630>) as the same document.	Y
3657	If an attempt is made to close an aggregation within the ERMS that includes a checked-out document, it must report this as an exception to an administrative role.	Y
2386	Users should be able to capture a document from within the EDMS.	Y
2385	Users must be able to transfer smoothly to and from the ERMS to declare the document as a record from within the EDMS.	N
3323	*This requirement is especially important where the EDMS/ERMS is used in a general office environment.*	
3418	Where there are multiple versions of a document the ERMS must be able to capture the document as a record in all of the following ways, with one being selected as default at configuration time and the user being able to select one during capture:: • the most recent version; • one version that is specified by the user; • all versions stored, held as a single record; • all versions stored, held as separate but linked records.	Y
3594	The ERMS must maintain a version number for each document, and must make it clearly visible when the document is retrieved or searched for.	Y
3595	The ERMS must automatically increment the document version number when a document is checked in as a new version.	Y
3596	The ERMS should allow the version numbering scheme to be defined at configuration time, allowing at least the following options; • simple sequential version numbering, that is numbers of the form 1, 2, 3; • major and minor version numbering, that is that is numbers of the form x.y., where x is a major version and y a minor version, with the user deciding whether to increment the major or the minor version, and the minor version being reset automatically to 0 when the major version is incremented.	Y
4590	*Other numbering schemes are acceptable.*	
3700	The ERMS must allow document version storage to be configurable by an administrative role, at configuration time or later, at class and file level within the classification scheme, with at least the following default options for each class and file: • all versions of all documents are stored in the class or file; • only the most recent version (where an administrative role has the ability to specify major or minor versions) of each document is stored in the class or file; • a number of versions of each document are stored in the class or file, the number being specified by an administrative role.	Y
3701	*This is to enable version control to be used where a history of document development is required. In areas where this history is not required, the number of versions stored - and hence the storage required - can be reduced.*	
3702	The ERMS should allow users who are storing a document to override the default value for the number of versions (as defined by <ID3700>) to be stored for that document.	Y

ID	Text, Requirement & Rationale	Testable
981	**10.4 Document Management and Collaborative Working**	
3324	*For example, the time of creation and author of a document, also metadata identifiable from structured fields within documents if these exist, such as date and subject.*	
3415	The ERMS allow a user to enter metadata values for a record at the time of capture.	Y
3416	The ERMS must ensure that any metadata that is captured is managed in accordance with the MoReq2 metadata model.	Y
3419	Where there is any conflict in the metadata between the ERMS and the document-generating system, the ERMS must alert the user.	Y
3648	*This can arise when the ERMS does not have control over the metadata elements in the document.*	
2383	The ERMS should be capable of integration with new EDMS versions or systems as these are brought into use by the organisation.	N
3588	*MoReq2 does not specify how this is achieved. Organisations should consider specifying this capability in more detail.*	
2380	The ERMS must be capable of version control, that is managing different versions of an electronic document as a single entity.	Y
3417	*This supports the drafting process of a document and enables collaborative working*	
2379	The ERMS should be able to restrict users to viewing: • only the latest version of a document; • selected versions of a document; • all versions of a document; • versions that have been captured or registered as records, the choice to be made at configuration or a later time by an administrative role.	Y
2378	The ERMS should be able to interface with related packages, including image processing and scanning systems (see section 6.7), and workflow systems (see section <10.5>).	P
3422	The ERMS should allow users to have a 'personal' workspace for documents.	Y
3593	*This can be used by users to store personal documents which are not expectedt to be captured as records, for example, early drafts which are not suitable for corporate access, or other documents. The use of this workspace should be optional*	
4658	Where the ERMS includes personal workspace, an administrative role must be able to limit the size of this on a per user basis.	Y
4659	Where the ERMS includes personal workspace, access of this must be restricted to the owner.	Y

10.5 Workflow

ID	Text, Requirement & Rationale	Testable
1031	**10.5 Workflow**	
1032	The Workflow Management Coalition (WfMC) - an international association for developing workflow standards and interworking of different workflow systems - defines workflow as "The automation of a business process, in whole or part, during which documents, information or tasks are passed from one participant to another for action, according to a set of procedural rules." In this definition, a "participant" can be a user, a work group (i.e. a team), or a software application.	
4352	As stated in <ID4351 in section 6.1>, the ERMS should provide basic workflow facilities to enable simple routing for checking and approving a document before registration and recording who took the decision, when and for what reason.	

ID	Text, Requirement & Rationale	Testable
1031	**10.5 Workflow**	
1033	The requirements in this section cover both basic routing functions, as described above, and more sophisticated workflow facilities including handling high volume transactions with exception cases, and reporting on system and individual performance. The latter may be provided by integrating a third party workflow product with the ERMS.	
1034	Workflow technologies transfer electronic objects between participants under the automated control of a program. In the context of ERMS, workflow is used to move electronic files and/or documents and records between users, departments and application programs. It is commonly used for: • managing critical processes such as registration and disposition procedures of files or records; • checking and approval of records before registration; • routing records or files in a controlled way from user to user for specific actions e.g. check document, approve new version; • notifying users of the availability of records; • distribution of records; • to manage records through case work processes.	
2390	**Requirement**	
2412	The ERMS must allow workflows which consist of a number of procedural steps, each step being (for example) movement of a document, record or file from one participant to another for action or decision.	Y
2408	The ERMS must allow pre-programmed workflows to be defined by administrative roles.	Y
3599	The ERMS must allow administrative roles to save workflows for future use.	Y
3600	*This implies that each saved workflow is assigned a unique identifier.*	
2407	The ERMS must restrict amendment of pre-programmed workflows to administrative roles, or authorised users.	Y
3598	The ERMS should allow the automatic declaration of a document to be a step in a workflow.	Y
3601	The ERMS should allow the administrative role storing the workflow to assign a unique textual title to it.	Y
3602	Whenever an administrative role changes and stores a workflow, the ERMS should store a copy of the workflow before the changes as a record, and should automatically assign a new version number to the changed workflow, with metadata specifying the date/time interval during which it was in effect.	Y
2403	The ERMS must not limit the number of workflows which can be defined and stored.	P
3604	The ERMS should allow user roles to define, use and save immediately new, personal, workflows (sometimes called *ad hoc* workflows).	Y
3438	The ERMS should include a graphical interface to enable administrative and user roles to define, maintain and edit workflows.	Y
2411	The ERMS should not limit the number of steps in each workflow.	P
3435	The ERMS must support the definition of distinct workflow roles to different users.	Y
4354	*Examples of these roles include:* • *a workflow administrative role (having permissions to reassign tasks or actions to another user or workgroup);* • *a supervisor role (having permissions to designate a workflow for exception handling in a specific case);* • *ordinary workflow users or workgroups.*	
3436	*These workflow roles are distinct from the ERMS roles set out in chapter 13.4.*	

ID	Text, Requirement & Rationale	Testable
1031	**10.5 Workflow**	
3437	The ERMS should enable an administrative role to define the maximum number of steps in a workflow at configuration time.	Y
2393	The ERMS should allow the administrative role defining a workflow to associate time limits with individual steps, and report items which are overdue according to these limits to a nominated user or administrative role.	Y
4353	The ERMS should allow the administrative role defining a workflow to choose from a pre-defined list which actions shall be taken by the participants of the workflow.	Y
4355	The ERMS should allow the administrative role defining a workflow to choose the participants: • by name; • by roles; • by organisational units.	Y
3603	The ERMS must allow user roles to initiate (i.e. use) workflows defined by administrative roles.	Y
2410	The ERMS must alert a user participant when a file or record(s) has been received in the user's electronic "in tray" for attention.	Y
3605	*MoReq2 does not specify whether this in tray is the participant's e-mail account in tray, or separate from it.*	
3328	The ERMS should support tracking of files and records by the provision of bring forward (also referred to as "tickler") facilities which enable a user to request a reminder to access the file or record on a future date.	Y
2409	The ERMS must provide a mechanism to allow users to notify other users of records requiring their attention.	Y
3425	*This may use an existing e-mail system or a standalone or proprietary messaging system.*	
2406	Administrative roles should be able to allocate permissions to individual users so that they are able to reassign tasks/actions in a workflow to a different user or group.	Y
3426	*A user may wish to send a file or record to another user because of the record content, because the assigned user is on leave, or for other reasons.*	
2405	The ERMS must record all creation of, and changes to, pre-programmed workflows in the audit trail.	Y
2404	The ERMS must allow users to monitor the progress of workflows they initiate and in which they are participants.	Y
3430	The ERMS must ensure that all records and files retain any links during a workflow process.	P
2402	The ERMS should manage the files and records in queues which can be examined and controlled by administrative roles.	Y
2401	The ERMS should enable participants to view queues of work addressed to them and either should • select items for action; or • present items for attention on a first-in-first-out basis; the option to be specified when the workflow is designed.	Y
2400	The ERMS should provide conditional flows depending on user input or system data to determine the direction of the flow.	Y

ID	Text, Requirement & Rationale	Testable
1031	**10.5 Workflow**	
3427	*In other words, flows which take the record or file to one of a number of participants depending on a condition decided by one of the participants. For example, a flow may take a record to either a credit control participant or an order consolidation section, depending on input from a sales supervisor; or the flow may depend on the value of an order, as computed by the system.*	
2398	The ERMS should allow users to suspend a flow temporarily in order to be able to attend to other work, and to resume it later (including after logging off from the system).	Y
2397	The ERMS must recognise as "participants" both users and work groups.	Y
2396	Where the participant is a work group, the ERMS workflow feature should include a facility to distribute incoming items to group members in rotation, or on a member's completion of the current task, to balance team members' workloads.	Y
2395	The ERMS should be able to prioritise items in queues.	Y
2394	The ERMS should include "rendezvous" processing.	Y
3428	*This requires the workflow to be paused to await the arrival of a related electronic document or record. When the awaited item is received, the flow resumes automatically.*	
4656	The ERMS should include the ability to trigger an instance of a specified workflow automatically when a record of a specified record type is received.	Y
4657	*For example, a loan application workflow can be triggered automatically by the receipt of a record with record type "loan application form".*	
2392	The ERMS should allow the receipt, in specified folders, of electronic documents or records to trigger workflows automatically (the workflow being determined by the document type or other metadata value).	Y
2391	The ERMS must provide comprehensive reporting facilities to allow management to monitor quantities, performance and exceptions.	Y
3439	The ERMS should support the capture of a workflow process as a record.	Y
3608	When file(s) or record(s) have been processed using one or more workflows, the ERMS must allow users to determine the identifier(s) and the version(s) of the workflow(s) used.	Y
2202	The ERMS should support the disposition, review and export/transfer process, by tracking and reporting on: • progress/status of the review, such as awaiting or in-progress, details of reviewer and date; • records awaiting disposition as a result of a review decision; • progress of the transfer process.	Y
3433	The ERMS must notify an administrative role if a record or file within a workflow is scheduled for review or disposition.	Y
3431	The ERMS must ensure that all access controls are maintained at all times.	P
3609	*In other words, it must not be possible to configure any workflow to grant any access to any user that the user would not otherwise have.*	
3434	The ERMS should be compatible with the Workflow Management Coalition Reference Model.	Y
3441	The ERMS should support the export of a standard workflow process or any of its constituent parts according to any standard XML schema(s).	Y
3610	The workflow audit trail should be integrated with the ERMS audit trail.	Y
3750	The workflow audit trail must be unalterable.	Y

10.6 Casework

ID	Text, Requirement & Rationale	Testable
2058	**10.6 Casework**	
2059	This section specifies requirements for the handling of "case files" in a MoReq2-compliant ERMS.	
3469	There is no universally-accepted definition of "case file", nor of the distinction between case files and the other kinds of files often managed by an ERMS. The following is therefore developed for, and intended to facilitate, the understanding of MoReq2; its applicability in other situations is not guaranteed.	
3484	The term "case file" is defined in the MoReq2 glossary as *a file relating to one or more transactions performed in a structured way.* In this context, "structured" means that the transactions follow rules that are (or that could be) documented, that they follow a consistent process (they do not allow for users to invent completely new parts of the process), and that they are repeated across many instances of similar transactions. The contents of the records in a case file may be structured (e.g. completed online forms) or unstructured (e.g. e-mail messages or scanned images of paper forms), in any combination; the key distinguishing characteristic of case files is that they result from processes which are structured, at least in part.	
3483	Examples of case files can include files containing records pertaining to: • regulatory monitoring: each case file contains the records relating to the process of monitoring an incident or company; • query and complaint management: each case file includes all the records relating to one query or complaint, and its resolution; • applications for permits, jobs, benefits, passes etc.: each case file contains the records relating to one application and the processes of approving the permit, paying the benefit, issuing the pass, etc.; • investigation of an incident: each case file contains the records relating to the investigation and resolution of an incident; • human resources: each case file contains the records relating to the recruitment, employment, and termination of an employee; • other transactions supported by a pre-programmed workflow (but not an ad hoc workflow created for a single use).	
3884	Typically, case files feature a predictable structure for the arrangement of the records they contain, albeit sometimes with numerous variations. For example, a Refund Request case file might always contain completed application forms, then either requests for clarification or approval documentation, and so on. Case files are often divided into sub-files (see Glossary) in a way that reflects this structure. Case management processes normally rely on business rules (implicit or explicit) which state that specified documents must automatically be considered as records.	

ID	Text, Requirement & Rationale	Testable
2058	**10.6 Casework**	
4567	By contrast, the content of non-case files is unpredictable, and is determined solely by the users who declare the records. Non-case files tend to contain records collected during a business process which does not follow formalised rules, which may be unique, and which can vary from file to file, and which can vary both according to the preferences of the individuals involves and the nature of the subject matter. Users who are working with non-case file documentation tend to decide whether a document should or should not be a record based on their experience and judgement, as opposed to the business rules that apply for case file documentation. Examples of non-case files might include records pertaining to: • an unexpected issue, that has to be resolved in a unique manner and for which there is no precedent; • collection and analysis of intelligence (whether related to a market or to security matters); • collaborative development of a new policy.	
3482	Typically, though not necessarily, other characteristics of case files are that: • they are numerous; • they are structured or partly structured; • they are used and managed within a known and predetermined process; • they need to be retained for specified periods, as a result of legislation or regulation; • they have similar content and/or structure; • they can be opened and (in many cases) closed by case-workers (practitioners, clerical staff or data processing systems) without the need for management approval.	
3885	Because case files often are structured, they often will contain several sub-files, usually configured by means of a template. They may also contain volumes. See section <3.3> for details of relevant functionality, all of which applies to case files as it does to other files.	
3481	Case management frequently involves another business application system which is external to the ERMS (sometimes called a "line of business" system) but which interfaces with it.	
3480	Examples of such systems include: • a licence application processing system; • an enquiry tracking system; • a human resources management system; • an order processing system.	
3478	A final differentiator is that casework files do not require a highly structured classification scheme. In most situations an essentially flat structure is appropriate for the case files of each kind of case. In these situations, the case files for a specific kind of case all are allocated to a single case work class, which itself is positioned in the classification scheme; each different kind of case typically is allocated to a different case work class, allocated elsewhere in the classification scheme.	
3886	Case working often depends on workflows. Requirements for the integration of workflows are described in section <10.x>.	
3477	**Requirement**	
3495	An administrative role must be capable of configuring the ERMS to allow at least one "case worker" role (see Glossary), with the specific feature that case worker roles can have different access permissions for case work classes and non-case work classes.	Y

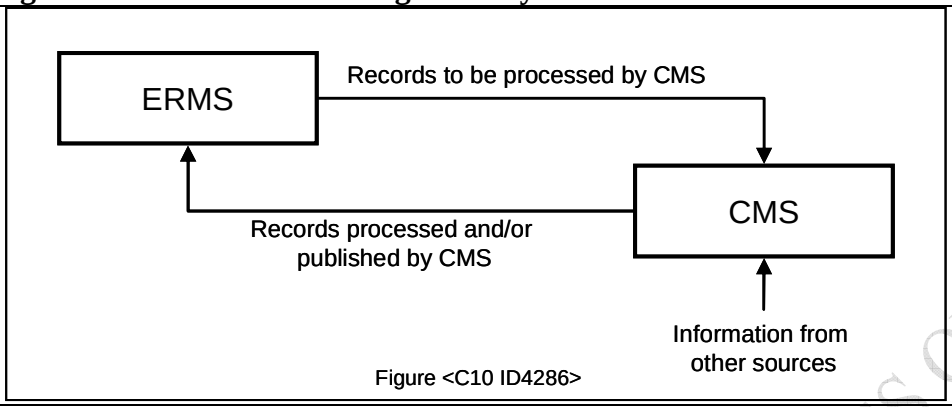
ID	Text, Requirement & Rationale	Testable
2058	**10.6 Casework**	
3496	*In many cases case workers will be able to create, open and close case files as part of their day-to-day business, but they will not have permissions to create, open and close non-case files. In non-case files this level of authority may be granted only to administrative roles.*	
2094	The ERMS should support an optional file titling mechanism, to be configured by an administrative role, which includes names (e.g. persons' names) and/or dates (e.g. dates of birth) or unique file identifiers as file names, derived and automatically validated from external lists.	Y
4640	The metadata used for automatically constructing file titles must be mandatory metadata or suitable defaults should be provided when the titling mechanism is defined. Where the underlying metadata (i.e. names, dates, etc.) which has been used to create the file title is modified, the ERMS should not automatically update the file's title.	Y
2669	*This requirement is appropriate for transaction processing environments. Any list used for validation may be managed within the ERMS or may be external to it.*	
4227	*Where a file title has been allocated automatically using a mechanism that incorporates metadata such as person's names, dates of birth, etc. it is possible for this original metadata on which the title is based to be updated. For example, a person's name may change, a date of birth may have been recorded incorrectly, etc. In these circumstances the file title based on the metadata should not be automatically modified to reflect the change as the file title may already have been used (e.g. in correspondence, registered on another system, etc.). Apart from the requirement that the file title is not automatically modified, MoReq2 does not mandate the possible outcomes.*	
4228	*Several different outcomes are possible, including:* • *the metadata change is ignored and the file title stays the same;* • *an administrative role is alerted that the metadata has been changed, and the role is able to (optionally) update the file title;* • *the user making the change is warned that the metadata has been used in the file title and asked to confirm the metadata change;* • *the user making the change is prevented from updating the metadata and advised to forward the desired changes to an administrative role who is able to edit the metadata.*	
3476	The ERMS must allow the creation of case files by any user authorised as a case worker.	Y
3497	The ERMS must allow entry of a case-specific file identifier.	Y
3474	*In most case files the file identifier, i.e. title or reference number will be provided by an external system. An interface should enable the user to validate a manually entered identifier against this.*	
2748	The ERMS must provide an Application Programming Interface (or comparable capabilities) to enable integration with other business applications. This must include at least the following functionality: • the other business application to create, open and close ERMS case files; • the other business application to provide the ERMS case file title; • the classification code of a newly-created case file to be passed to the other business application; • the other business application to pass records to be declared into the ERMS case files; • the other business application to apply a retention and disposition schedule to an existing closed file; • error handling in case either system initiates an action which is considered invalid by the other system.	P

ID	Text, Requirement & Rationale	Testable
2058	**10.6 Casework**	
4356	*It is as if the business application should act as a normal user - the ERMS should not differentiate between the two.*	
3493	• *MoReq2 does not specify the nature of the error processing. However, specific outcomes are identified in the following two requirements.*	
4568	*The ERMS must, upon receipt of an apparently invalid request from an external business application:* • *not complete any invalid action;* • *not result in a software failure in either the ERMS or the external application.*	
4569	*The ERMS should, upon receipt of an apparently invalid request from an external business application alert an authorised user so that corrective action can be taken.*	
3887	Where the ERMS interfaces with another business application it must be possible for an administrative role to limit the other application's actions to one or more specified classes within the ERMS classification scheme.	Y
3888	*In other words, it must not be possible for the other application to take any actions that affect class, files or records beyond the class(es) for the case files.*	
3499	Where the ERMS interfaces with another business application it should be possible for a user to switch easily between the related files in both applications.	N
3889	*In other words, a user that has used the features of the other business application to locate or identify a case or case file (for example, using the application's postal address look-up features to identify a specific case) must be able to open that case file in the ERMS easily, that is without having to re-type the case file identifier. Likewise, a user who has opened a case file in the ERMS (by browsing the classification scheme, by searching or by any other means) must be able to switch to the corresponding case information in the other business application in the same way.*	
3491	Where the ERMS allows another business application to create new case files it must be able to receive relevant file metadata from the other application.	Y
3490	The ERMS must allow case files to be configured with metadata elements that are specific to case files.	Y
3489	*For example, a case file may need one or more metadata elements to indicate "status" or "progress".*	
3890	The ERMS must allow users to retrieve, declare records into, and carry out all other valid actions on case files by using a case file identifier instead of a classification code.	P
3891	*Most case files are identified by a unique case identifier such as an account number or a complaint number. Users must be able to work with these files simply by specifying this identifier, and without the need to use the ERMS classification code (though use of the code will remain possible).*	
3892	When the ERMS receives records with structured content from another business application, it should be able to extract metadata automatically from the records.	Y
4163	When the ERMS receives records with structured content from another business application, it should be able to use the extracted metadata to declare the records into the appropriate file.	Y
3893	*For example, if an ERMS receives electronic claim forms from a benefits claim processing application, it should be able to extract the claimant identifier and form type, then use these to classify the forms to the correct case file (using the claimant identifier) and sub-folder (using the form type).*	
3894	-	
3487	The ERMS must ensure that all actions performed on any class, file, or record, whether by an authorised user or by another business application, are recorded in the audit trail.	Y

ID	Text, Requirement & Rationale	Testable
2058	**10.6 Casework**	
3486	The ERMS must be capable of producing reports on all actions performed on any specified file(s), whether by an authorised user or by another business system.	Y
3895	The ERMS must be able to produce reports for administrative roles, showing at a minimum: • the numbers of records declared into case files automatically from other business systems per time period; • the numbers of records declared into case files manually per time period; • the numbers of case files opened and closed automatically by other business systems per time period; • the numbers of case files opened and closed manually per time period.	Y

10.7 Integration with Content Management Systems

ID	Text, Requirement & Rationale	Testable
2060	**10.7 Integration with Content Management Systems**	
4282	This section addresses the requirements for the integration of "Content Management Systems" (CMSs) with ERMSs. Modern content management systems include most or all of electronic document management system (EDMS) functionality. Integration with EDMS is addressed in section <10.4>; this section addresses only the CMS-specific requirements. It describes the functional requirements for an ERMS only - it does not describe the functional requirements for CMSs, and does not include sufficient functionality to make the ERMS perform tasks normally associated with CMSs.	
4574	While CMS includes EDMS functionality, it extends further. The choice of the word "content" indicates that CMS aims to extend across all forms of information (content), not just records.	
2061	There are many definitions of CMS. Most or all of them involve the management of digital information using a software system. CMSs usually deal with different aspects of managing information than ERMSs. Frequent characteristics of CMSs are: • publishing information, often to websites or portals, and sometimes to several channels using different renditions; • managing information that originates from several sources; • reformatting information and/or migrating it to some different rendition(s); • relating different versions, renditions and translations of documents to each other; • managing components of documents.	
4289	At the time of writing, the most frequent use of the term CMS, and the most frequent need for integration with an ERMS, is likely to apply to web publishing. However, this section is intended to allow for both web publishing and other sorts of CMS.	
4288	Content management functionality may be provided by a CMS separate from the ERMS, or by an integrated package that provides both CRM and electronic records management functionality. For ease of explanation, this section describes MoReq2 requirements as if the CMS and ERMS are separate; this separation is not a requirement.	
4287	The relationship between an ERMS and a CMS is shown, in highly simplified form, in the following figure.	

ID	Text, Requirement & Rationale	Testable
2060	**10.7 Integration with Content Management Systems**	
4286	 Figure <C10 ID4286>	
4284	This figure shows that: • Copies of records can be passed from the ERMS to the CMS for processing (the processing usually involves editing, migrating to different renditions, and publication). • Documents can be passed from the CMS to the ERMS for capture. This can happen while information is being processed by the CMS, or after it has been processed and published by the CMS. These may take many forms, including (though not limited to) web pages, web sites, and new renditions of existing records. • The CMS can also receive information from other sources, so the documents it passes back to the ERMS can consist of a combination of information that originated from the ERMS and information from elsewhere.	
4290	Note that the words " can be passed to…" cover several possibilities: • copies of the documents or records are transmitted between applications; • they are stored in a repository that is common to the CMS and the ERMS, and only messages identifying the documents or records are transmitted between the applications; • possibly other scenarios.	
4283	For simplicity, this figure shows only the relationships that are relevant to these requirements. Thus it does not show other inputs of the ERMS, publication outputs of the CMS, etc.	
4267	CMS technology is evolving rapidly, so organisations that require CMS integration must specify their individual requirements; reliance on this section alone is not likely to suffice. This section should be viewed as a starting point, to prompt further analysis.	
4270	**Requirement**	
4291	The ERMS must allow users to initiate the passing of copies of specified records, together with at least some of their metadata, from the ERMS to the CMS.	Y
4292	*The metadata to be passed can be specified at configuration time.*	
4294	The ERMS must be able to receive as input from the CMS documents, including some metadata, and must either: • automatically declare the records into the appropriate file(s) based on their metadata; or • allow a user to specify the appropriate file(s).	Y
4265	The ERMS must accommodate metadata required by the CMS in addition to the records management metadata specified by MoReq2.	Y

ID	Text, Requirement & Rationale	Testable
2060	**10.7 Integration with Content Management Systems**	
4272	*For example, a CMS may use metadata elements to store information needed for content management, such as:* • *IP address;* • *status;* • *language;* • *publication date;* • *effective date;* • *reason for change.* *The ERMS must be able to store these elements, even though they are not required for records management. It is not necessary for the ERMS to be able to store all the metadata produced or used by the CMS; only the elements specified at configuration time need be stored. The elements to be stored need to be determined based on business need.*	
4296	*Note that this is a highly general requirement. It allows for a wide variety of functions to be carried out by the CMS then recorded as metadata stored in the ERMS.*	
4297	When a user is selecting records to copy from the ERMS to the CMS, the ERMS must allow the user to use the CMS metadata values as a basis for selecting the records to be passed.	Y
4298	*Continuing the example in <ID 4272 above>, a user may select records in a specified class with specified values of "effective date" and "status".*	
4299	When a document is being passed from the CMS to the ERMS for capture, if that document is related to an existing record stored in the ERMS (for example, it is a different rendition or a translation of the existing record), the ERMS must not delete or change the existing record, but must instead store the new record.	Y
4273	When a document related to an existing record (as in <ID4299 above>) is being passed from the CMS to the ERMS for capture, the ERMS must automatically link the existing and the new records (as in <IDxxxx on linking records together>).	Y
4300	*This will only be possible if the CMS passes, with the document, the identifier of the existing record, as a metadata value. If the CMS does not pass back this value, then the ERMS cannot fail a MoReq2 compliance test by not meeting this requirement.*	
4259	When a document related to an existing record (as in <ID4299 above>) is passed from the CMS to the ERMS and then captured as a record, the ERMS should ensure that the metadata of the new record is as far as possible identical to that of the original record by binding it to the same metadata, with only such relevant differences in the metadata as are required to record the changes and actions of the CMS.	N
4253	When documents are being passed from the CMS to the ERMS in the form of web pages, the ERMS should be able to capture a web page, or a set of web pages, declaring them as a single record.	Y
4302	*The ability to capture a set of pages as a single record may be useful in several circumstances, such as storing "snapshot" copies of a web site periodically.*	
4303	*Capturing web pages is likely to require changes to the references (hyperlinks within the pages, hyperlinks to other web pages, and references to graphical or other components etc.) so as to allow the pages to appear correct and to retain as much as possible of their original functionality. This is contrary to the general principle of not changing the content of records, but is unavoidable if web pages that include graphical elements, style sheets, hyperlinks etc. are to be stored in their original formats without losing all functionality and fidelity. See requirements <section 6.2 ID4636 and ID4638>.*	
4305	When records are being passed from the ERMS to the CMS, this must be recorded automatically in the ERMS audit trail and in the records' metadata.	

ID	Text, Requirement & Rationale	Testable
2060	**10.7 Integration with Content Management Systems**	
4301	When documents are being received by the ERMS from the CMS, this must be recorded automatically in the ERMS audit trail and in the records' metadata.	Y

10.8 Electronic signatures

ID	Text, Requirement & Rationale	Testable
1089	**10.8 Electronic signatures**	
1090	Electronic signatures (sometimes referred to as digital signatures) are sequences of characters which are used with secure algorithms procedures and "keys" (a long string of digits analogous to a password) to confirm the integrity of a record, or to authenticate the identity of the sender or the source of a record. Electronic signatures should not be confused with a bitmap, or scanned image, of a manual "pen and ink" signature on paper – this is not considered secure, and so is unlikely to add to the evidence about authenticity of a record.	
4582	An electronic signature, as the term is used in MoReq2, is a form of "advanced electronic signature" as defined in the European "Directive on a Community Framework for Electronic Signatures" 1999/93/EC. The most commonly recognised standard for such frameworks is X.509 (see appendix 7.1).	
4575	Examples of widely-recognised electronic signature algorithms are the Secure Hash Algorithms such as SHA-1 which have largely superseded the earlier MD5 (Message-Digest algorithm 5).	
1091	e-Mail has become the default means of communication for many organisations and this has resulted in the widespread movement of documents and records in relatively uncontrolled environments. The use of electronic signatures for authentication and integrity confirmation is therefore becoming widely adopted, especially where records of business transactions are involved.	
3411	Electronic signatures are also used to provide non-repudiation. For example, the sender of an electronically signed e-mail cannot refute that he is the originator of the message provided his electronic signature can be proved to be valid at the moment of signing.	
1092	The requirements in this section apply only where there is a requirement to manage records bearing electronic signatures. At the time of writing, electronic signatures are still subject to change and uncertainty as new infrastructures and algorithms are tested and introduced. This state of affairs is likely to continue to evolve for the foreseeable future. Users of MoReq2 should therefore confirm requirements and implications for long-term storage with appropriate authorities.	
3412	There are no requirements in this section relating to individual countries' legislation on electronic signatures. By way of illustration, some laws require that a signature be retained complete to have value, while others require only the retention of metadata about a signature. Where these are relevant they may be dealt with in a country-specific chapter zero.	
2413	**Requirement**	
2420	The ERMS must be able to capture, and store, at the time of record capture, electronic signatures, associated electronic certificates and details of related verification agencies.	Y
3614	*This is essential as it will not always be possible to recreate this information at later times.*	

ID	Text, Requirement & Rationale	Testable
1089	**10.8 Electronic signatures**	
3305	The ERMS must enable administrative roles to configure the system, either at configuration time, or at a later date, to store verification metadata for electronically signed records, including public keys, with the record at time of capture in one of the following ways: • the fact of successful verification; • specified information regarding the verification process; • all verification data.	Y
3615	*This is essential as it will not always be possible to recreate this information at later times.*	
2419	The ERMS should have a standards-based interface which permits the introduction of new electronic signature technologies as they are introduced.	N
4642	*An example of a suitable standard basis is the XML Key Management Spec (XKMS, see Appendix 7.1).*	
3302	*This is especially valuable given the changes occurring in this area.*	
2418	The ERMS should be capable of checking the validity of an electronic signature, including checking the certificate against a Digital Certificate revocation list, of a record at the time of capture and storing.	Y
3616	*This is valuable as it may not always be possible to perform this check on the information at later times.*	
2417	When capturing e-mail messages the ERMS must be able to capture automatically and preserve as metadata, details about the process of verification for an electronic signature, including: • the fact that the validity of the signature was checked; • the serial number of the digital certificate, verifying the signature; • the Certification Authority with which the signature has been validated; • the date and time that the checking occurred.	Y
3617	*This is essential as it may not always be possible to recreate this information at later times. Because software changes, because certificates expire, and because external authorities can cease to exist, electronic signatures cannot be relied on over long periods; hence this requirement to record the fact that a signature was successfully verified.*	
2415	The ERMS should include features which demonstrate that the integrity of records bearing electronic signatures has been maintained.	N
3306	*An example of this would be the verification of an electronic signature. This demonstration of integrity should apply even if an administrative role has made authorised changes to the metadata of the record.*	
3303	*The way in which this might be achieved is not prescribed.*	
2414	The ERMS should be able to store with the electronic record: • the electronic signature(s) associated with that record; • the digital certificate(s) verifying the signature; • any confirming counter-signatures appended by the certification authority in such a way that they are capable of being retrieved in conjunction with the record.	Y
3314	The ERMS should enable administrative roles to apply an electronic signature to a file or record during an export process so that the file or record's integrity and origin can subsequently be verified.	Y
3315	An electronic signature applied during export (see <ID3314>) should be capable of external validation so that the file or record's integrity and origin can subsequently be verified.	Y

ID	Text, Requirement & Rationale	Testable
1089	**10.8 Electronic signatures**	
4357	*To do this the ERMS must be capable of exporting an electronic certificate with the organisation's public key, with the record.*	

10.9 Encryption

ID	Text, Requirement & Rationale	Testable
1110	**10.9 Encryption**	
1111	Encryption is the process of applying a complex transformation to an electronic object so that it cannot be rendered by an application in a readable or understandable form unless the corresponding decryption transformation is applied. This can be used to secure electronic objects, by use of transformations which require the use of secure electronic key codes.	
1112	The requirements in this section apply only where there is a requirement to manage records which are encrypted.	
2421	**Requirement**	
2426	Where an electronic record has been sent or received in encrypted form by a software application which interfaces with the ERMS, the ERMS must be capable of restricting access to that record to users listed as holding the relevant decryption key, in addition to any other access control allocated to that record.	Y
4095	The ERMS must be able to capture and store, at the time of record capture, information relating to encryption and details of related verification agencies.	Y
2425	Where an electronic record has been transmitted in encrypted form by a software application which interfaces with the ERMS, the ERMS should be able to keep as metadata with that record: • the fact of encrypted transmission; • the serial number of a digital certificate (where appropriate); • the type of algorithm; • the level of encryption used; • the date and time of the encryption and/or decryption process, where applicable.	Y
2424	The ERMS should be able to ensure the capture of encrypted records from a software application which has an encrypting capability.	Y
2423	The ERMS should allow encryption to be removed when a record is imported or captured. This feature should be configured by an administrative role at configuration time or later.	Y
3304	*This feature may be desired in some large scale record archives which have a requirement for long-term access (because encryption etc. is likely to reduce the ability to read records in the long term). In this case, the organisation would rely on audit trail or similar information to prove that the encryption etc. had been present but has been removed. In other environments, this feature may be undesirable from a legal point of view. See <insert reference here> for more details on Transfer and Importing.*	
2422	The ERMS should have a structure which permits new encryption technologies to be introduced.	N

10.10 Digital Rights Management

ID	Text, Requirement & Rationale	Testable

1126	**10.10 Digital Rights Management**	
3619	This optional module does not contain any requirements that are testable in their current form. As explained below, testing will be meaningful only when the requirements are adapted to specified technologies.	
1127	Digital Rights Management (DRM) and Enterprise Digital Rights Management (sometimes abbreviated to E-DRM) constitute a not yet standardised set of technologies used to protect intellectual property and/or to restrict the distribution of information. DRM is generally associated with the protection of intellectual property (especially in the music, electronic publishing and film industries), while E-DRM is generally associated with placing restrictions on the distribution of business information, for reasons of security or commercial sensitivity. However, the boundaries are not firm and either may be encountered in the context of an ERMS. Accordingly, in the remainder of this section these technologies are referred to as DRM/E-DRM.	
3620	Examples of DRM/E-DRM include: • Electronic watermarking (also referred to as digital watermarking), which imposes visible information about intellectual rights over electronic documents or records. The information is imposed in a complex manner that makes its removal difficult without the correct algorithm and key. • Steganography, which similarly imposes information about intellectual rights, but in a way that is invisible or, in the case of an audio file, inaudible. Special software is required to read the intellectual rights information. • Copy protection schemes, which use a variety of approaches to prevent copying. • Features built into documents or records that allow them to be viewed on-screen but not to be printed. • Expiry features built into documents or records that prevent them from being rendered in any way after a specified date has passed.	
3621	DRM/E-DRM technologies are at a relatively early stage of development. They are likely to change significantly during the expected lifetime of MoReq2.	
3311	These, and similar technologies, can be applied to records in many formats, including digitised sounds and moving pictures.	
3312	These technologies provide a particular challenge in records management as they may make future presentation of records difficult or, in some cases impossible. For example: • Some forms of watermark rely on the presence of "plug-in" software in the viewing application to be wholly effective. A record with such a watermark may be viewable without the plug-in, but it will not be possible to obtain all the watermark information if the plug-in is not available. As time passes the likelihood increases that the plug-in will not be available. • An e-mail message contains an expiry feature, and so will no longer be readable after a specified date. This problem is particularly insidious as it may not be apparent at the time the record is captured.	
3622	At a minimum, user and administrative roles responsible for capturing and managing electronic records should be aware of any DRM/E-DRM features affecting records in the ERMS. Additionally, potential records management difficulties caused by these technologies can be minimised if the DRM/E-DRM features are removed from records at (or around) the time of their capture. However, both of these points are procedural issues, and therefore beyond the scope of MoReq2.	

1128	The applicable technologies vary widely, and their effect on records varies equally widely. For this reason, it is not feasible to formulate generic requirements that apply to all the technologies. Therefore this section specifies some high-level requirements that must be made more specific by users of MoReq2 if they are to be used for specification and procurement. So, for example, if time-related expiry features are expected, the requirements must be adapted to give specific requirements for dealing with the expiry features.	
2427	**Requirement**	
2428	The ERMS must be capable of capturing and storing records bearing DRM/E-DRM features.	N
4359	The ERMS should be able to identify the presence of DRM/E-DRM features in a record at the time of capture. Where DRM/E-DRM features are identified, the ERMS should inform the user and provide the following options; • keep the DRM/E-DRM features; • remove DRM/E-DRM features if possible; • stop the capture process.	N
3626	The ERMS should be able to remove DRM/E-DRM features from records during capture.	N
3627	*This may be mandatory in some environments, but cannot be mandatory in the general case as it would require an arbitrary ability to circumvent security features. If DRM/E-DRM features are removed this should be recorded in the audit trail.*	
2299	The ERMS should include the ability to control access to records based on intellectual property restrictions, and generate charging data for such accesses.	N
3767	*This brief statement encompasses a wide range of functionality which is beyond the scope of MoReq2. This requirement may be satisfied by providing the ability to link to a separate application.*	
3623	The ERMS must be capable of correctly presenting records with DRM/E-DRM features, to the extent that the DRM/E-DRM features permit.	N
2429	The ERMS should be able to retrieve and store at the time of declaration, information stored in the DRM/E-DRM features, to the extent that the DRM/E-DRM features permit.	N
3624	*For example, the identities of the owners of the intellectual property, as encoded in a watermark; or an expiry date.*	
3625	*This may be mandatory in some environments, but cannot be mandatory in the general case as it would require an arbitrary ability to circumvent security features.*	
2430	The ERMS should allow new DRM/E-DRM technologies to be introduced.	N
3316	The ERMS should be able to apply DRM/E-DRM features to records during export.	N
3317	*This is especially desirable if a DRM/E-DRM feature has been removed.*	

10.11 Interoperability and Openness

Note to reviewers: The expected contents of this section have been absorbed into other sections, notably those on capture, metadata, and case work. Also, the requirements are not optional in the sense of constituting an optional module. We therefore expect to delete this section in future drafts. This heading is retained in this draft for numbering purposes only.

10.12 Distributed Systems

ID	Text, Requirement & Rationale	Testable
2062	**10.12 Distributed Systems**	
2063	This section comprises requirements for organisations that require an ERMS to operate in multiple locations.	

ID	Text, Requirement & Rationale	Testable
2062	**10.12 Distributed Systems**	
4140	Many organisations operate from several sites. Where the sites are relatively close to each other geographically, or when the network connection between all the sites is good (with sufficient capacity) then it may be that a single "instance" of an ERMS is most appropriate to cope with all sites; in this case, all the sites operate as if they were co-located, and the requirements of this section need not apply. However, if the sites are widely separated, and/or if the connectivity between them is not good, then it may be necessary to implement a distributed ERMS; in that case the requirements in this section apply.	
4316	There are several different architectural approaches to distributed systems. These include one instance of an ERMS controlling multiple repositories; several instances of an ERMS, each with its repository(ies), communicating with each other; and other approaches. MoReq2 does not specify an architectural approach; it specifies only the key requirements for such distributed environments; it uses the term "distributed ERMS" to refer to any such architecture.	
3177	**Requirement**	
4145	The ERMS must be capable of being configured by an administrative role for use across multiple locations.	N
2083	The ERMS should support a distributed classification scheme across a network of electronic record repositories.	Y
3529	The ERMS must allow an administrative role to maintain classes, files, sub-files, volumes and records and their associated metadata and audit trails across the distributed ERMS such that maintenance operations can be carried out once to apply to the entire distributed ERMS.	P
4317	*Maintenance means performing transactions as specified in chapter 3, section 9.1 and elsewhere.*	
4318	Where the ERMS supports multiple repositories, it should allow an administrative role to specify which repository stores the 'master' copy of each class (and its descendant classes, records classified to it, etc).	Y
4319	*For example, an organisation may decide to implement one repository for each of its locations, with each location's records being stored in the location's repository (this assumes that the classification scheme design supports this configuration).*	
4320	Where the ERMS supports multiple repositories, it should allow an administrative role to specify which repository(ies) automatically store a copy of each class (and its descendant classes, records classified to it, etc.).	Y
4321	*For example, an organisation may decide that:* • *all repositories have to be copied to the head office repository;* • *in one territory, all repositories must be copied to each other.*	
4322	*Note that this implicitly means that repositories need to be synchronised automatically. This includes the repositories':* • *records and documents;* • *metadata.*	
4323	Where the ERMS supports multiple repositories, it should allow an administrative role to specify which repository(ies) the users at each location can access.	Y

ID	Text, Requirement & Rationale	Testable
2062	**10.12 Distributed Systems**	
4324	*For example, an organisation may decide that:* • *all users can access only the repository for their location;* • *all users can access the repository for their location and the head office repository;* • *all head office users can access any repository while all other users can access only the repository for their location;* • *all users can access all repositories within their territory (i.e. within a specified set of repositories; this is not intended to imply that the ERMS has to recognise the concept of 'territory').*	
4325	Where the ERMS supports multiple repositories, it should allow an administrative role to specify that all audit trails will be copied to one repository.	Y
3531	The ERMS must prevent or resolve any conflicts caused by changes made in different locations.	P
4327	*For example, a potential conflict may arise if two administrative roles in different locations make a different change to the metadata of the same class which is stored in a third location.*	
3530	The ERMS must allow an administrative role to monitor both the entire distributed ERMS as a single entity and individual repositories, providing the same facilities as described in section <9.2>.	Y
4148	The ERMS should be able to produce reports (as specified in section <9.2>) that cover multiple repositories.	Y
3532	The ERMS should support caching of frequently and recently used files, sub-files, volumes and records accessed from locations using remote repositories.	Y
3534	*The following two requirements relate to the performance of the distributed ERMS. They use the convention of expressing variable quantities in angle brackets (for example <xx minutes/hours>) as explained in the introduction to chapter 11.*	
3535	Where the ERMS synchronises repositories, they must be synchronised within <*xx* minutes/hours> of any change (subject to availability of network connections).	N
3533	The ERMS must be capable of propagating any administrative change across all repositories within <*xx* minutes/hours>.	N
4152	*Requirements <ID3535 above> and <ID3533 above> are example requirements. MoReq2 does not specify response times as these will be system dependant. See chapter 11.2 for a full description.*	
4146	*It is critical that the system architecture allows acceptable response times across all locations. Users of MoReq2 should consider specifying response times for many of the requirements specified in section 11.2 separately for transactions involving information held in remote repositories.*	
4143	Where the ERMS is capable of creating workflows across distributed systems, it must be able to interchange data across these systems to control the workflow process.	Y
4329	Where the ERMS supports multiple repositories, and where "master" copies are stored in specified repositories (see <ID4318 above>, it should allow an administrative role to change which repository stores the 'master' copy of each class (and its descendant classes, records classified to it, etc); when such a change is made, the ERMS must move the contents from the old location to the new location.	Y
4330	*This will be useful when creating or removing repositories, or when moving records to a different repository following geographical moves involving business functions*	
4331	Where the ERMS supports multiple repositories, it must allow an administrative role to add a new repository.	Y

ID	Text, Requirement & Rationale	Testable
2062	**10.12 Distributed Systems**	
4332	Where the ERMS supports multiple repositories, it must allow an administrative role to remove a repository.	Y

10.13 Offline and Remote Working

ID	Text, Requirement & Rationale	Testable
2064	**10.13 Offline and Remote Working**	
2065	The requirements in this section cover all types of mobile and offline usage of the ERMS by users who are not permanently connected to the ERMS (or to the network hosting it).	
3548	There are several possible scenarios including: • users who access the ERMS using portable computers (such as mobile, laptop, or notebook computers) or PCs that are connected to the ERMS intermittently; • users who connect to the ERMS remotely through a dial up connection, or any other connection with low bandwidth connection (e.g. for telecommuting or in a temporary location); • users who access the ERMS using other mobile devices such as PDAs or smartphones.	
3543	Portable computers can be used as normal workstations when connected to the ERMS. However users may need to be able to download and synchronise records and data so that they can work on them whilst offline.	
4043	To enable this functionality the ERMS needs to download not only records and aggregations but also their metadata. The ERMS will also need to synchronise all of the modified data when the user is next connected to the system.	
4044	In a similar way, portable computers can be connected intermittently to the ERMS, for example when they are used by telecommuters. When they are connected, the portable computer will need to synchronise with the ERMS. Once again there will be the need to download records etc, with the downloaded data being managed on the portable computer in between synchronisations.	
4045	PDAs, smartphones and other handheld devices can be used to view and access records, in many cases using a browser interface. Inherent limitations, such as a small screen and restricted performance, mean that in many cases such a device cannot offer the full functionality of a portable or fixed computer. However, such devices are often used for mobile e-mail, notes and calendar applications and there is therefore a necessity to synchronise these types of document with the central system.	
4306	MoReq2 does not specify requirements to allow mobile or offline users to maintain the classification scheme (e.g. the creation of new classes) and files (e.g. closing a file). It may be possible to develop systems that support such maintenance, and MoReq2 does not prevent this.	
3544	**Requirement**	
4307	The ERMS should allow an administrative role to specify classes containing information that cannot be downloaded by any user.	Y
4308	*This is a security provision to protect sensitive information from being downloaded and hence placed beyond the control of the ERMS.*	
3545	The ERMS must enable a user to download any aggregation or record(s) with accompanying metadata for the user to work on whilst not attached to the network.	Y

ID	Text, Requirement & Rationale	Testable
2064	**10.13 Offline and Remote Working**	
4223	The ERMS must track in its audit trail all activity on downloaded aggregations, records, and documents.	Y
3546	The ERMS should note in the aggregation, record or document metadata that the item has been downloaded for offline use.	Y
3547	The ERMS must enable the synchronisation of downloaded aggregations and records upon connection to the system.	Y
4309	*That is, it must update the metadata.*	
4224	The ERMS must update the audit trail with information on offline activity upon connection to the system.	Y
4107	The ERMS must allow a user to create records whilst offline and to register them later, when connected to the ERMS.	Y
4108	*If the record has been created offline then the ERMS must either:* • *when re-connected, prompt the user in the synchronisation dialogue to file it within the appropriate file, sub-file or volume;* *or:* • *when re-connected, file it automatically, using the class, file or sub-file specified by the user while disconnected (subject to validation).*	
4106	The ERMS must apply all access and security controls to remotely connected devices.	P
4310	*The ERMS must not provide any opportunity for portable devices to breach the security rules of the ERMS. For example, a user must not be able to download any information which he or she could not access online. However, MoReq2 recognises that once information has been downloaded to a device the ERMS loses control of it, and that security breaches in this scenario cannot be prevented by the ERMS.*	
4311	*The following four requirements apply only where the ERMS supports electronic document management, as defined in section 10.4. They use terminology defined in that section.*	
4312	The ERMS must allow a user to download documents with accompanying metadata for the user to work on whilst not attached to the network.	Y
4313	The ERMS must allow users the option of checking documents out when they are downloaded.	Y
4314	If a user checks out a document and works on it while not connected to the ERMS, the system must allow version numbering to be applied to the document.	Y
4315	If a user checks out a document and changes its version number while not connected to the ERMS, when the user reconnects to the ERMS it must allow the user to upload the revised document, and must at that time automatically check it in and record the changes and the new version number.	Y

10.14Fax Integration

ID	Text, Requirement & Rationale	Testable
2068	**10.14 Fax Integration**	
4097	While e-mail has taken over from facsimile as many organisations' preferred method of rapid communication, there are still some occasions and some locations for which fax is required.	

ID	Text, Requirement & Rationale	Testable
2068	**10.14 Fax Integration**	
4098	This can be, for example, where the original document is not in electronic format and a copy needs to be sent to another organisation, or where a visible representation of, e.g. a signature is required.	
4100	Some fax servers integrate with e-mail systems so that both incoming and outgoing faxes are dealt with as e-mail attachments. In this case the requirements in <section 6.4> apply.	
4099	Where an organisation's ERMS is integrated with a fax service the following requirements apply.	
3540	**Requirement**	
3536	The ERMS should provide an application programming interface (API) to enable it to interface with a fax server.	N
3537	The ERMS must be capable of storing faxes in standard formats, for example TIFF v6 image format with Group IV compression.	Y
3541	The ERMS must support the capture of faxes in an integrated way, so that the capture can be performed by a user from within the fax interface (if user an interface exists), without the user needing to switch to the ERMS.	Y
3539	The ERMS must be tightly integrated with the fax interface to enable users to fax any electronic record that they currently are viewing or working with in the ERMS, from within the ERMS (so long as the record can be presented as a two-dimensional image).	Y
4096	It must be possible for an administrative role to configure the ERMS so that it operates in one of the following ways when an ERMS user sends a fax: • it automatically captures the fax as a record; • it automatically prompts the user, giving the user an option to declare the fax as a record; • it takes no action (and thus relies on the user to initiate declaration if appropriate).	Y
4101	*Regardless of which way is chosen, it is acceptable for the ERMS to require the user to classify the record manually and enter metadata manually.*	
4102	It must be possible for administrative role to configure the ERMS so that it operates in one of the following ways when an ERMS user receives a fax: • it automatically prompts the user, giving the user an option to declare it; • it takes no action (and thus relies on the user to initiate declaration if appropriate).	Y
4103	*Regardless of which way is chosen, it is acceptable for the ERMS to require the user to classify the record manually and enter metadata manually.*	
3542	The ERMS should be capable of automatically extracting fax metadata elements from incoming faxes, as specified in chapter 12, for example: • title; • sender; • time and date; • recipient.	Y
4221	*This may be accomplished by means of a fax template, and is only relevant where faxes have a predictable internal structure.*	
4112	The ERMS should be capable of automatically populating fax metadata elements for outgoing faxes, as specified in chapter 12, for example: • title; • sender; • time and date; • recipient.	Y

ID	Text, Requirement & Rationale	Testable
2068	**10.14 Fax Integration**	
4222	*This may be accomplished by means of a fax template, and is only relevant where faxes have a predictable internal structure.*	
4104	The ERMS must allow a user who is capturing a fax to edit the title metadata element, in order to reflect the content of the fax.	Y
3538	The ERMS should be capable of providing a fax record type for both inbound and outbound faxes to enable a user to enter metadata.	Y

10.15 Security Categories

ID	Text, Requirement & Rationale	Testable
424	**10.15 Security Categories**	
425	Chapter 4 describes requirements for controlling access to aggregations and records by role and group. In some environments, such as those involving national security, healthcare, etc, there is a need to limit access further, using a scheme of security categories and security clearances.	
4113	These clearances take precedence over any access rights which might be granted using the features defined in chapter 4. The requirements in this section apply only in organisations which have this need.	
426	This is achieved by allocating one or more "Security Categories" to classes, files, sub-files, volumes and/or records.	
4115	The term "Security Category" is used in this specification to mean "One or several terms associated with a record which defines rules governing access to it." Note that this term is used expressly for this specification; it is not generally employed.	
427	Users can be allocated a single security clearance which prevents access to all aggregations or records which have been placed at higher security categories.	
428	Security categories can be made up of sub-categories. Some sub-categories are hierarchic in nature. Other sub-categories may be arranged differently, typically in a way which is unique to an organisation or sector.	
4116	MoReq2 describes in detail only the requirements for a hierarchic sub-category.	
3523	The examples given here are based on national security markings but the same principles apply to markings used in other sectors.	
4114	There can also be country-specific national security classification requirements. Where appropriate these can be addressed in chapter zero.	
2167	**Requirement**	
2178	The ERMS must allow one of the following options to be selected at configuration time: • security categories are assigned to classes, files, sub-files and/or volumes (and not to individual records); • security categories are assigned to individual records (and not to classes, files, sub-files and/or volumes); • security categories are assigned both to individual records and to classes, files, sub-files and/or volumes.	Y
3504	*Some organisations will wish to control sensitive records individually, while others will wish to control them at the class, file etc. level.*	
4333	The ERMS must allow an administrative role to specify, at configuration time, which roles can specify and change the security category of records, classes etc.	Y

ID	Text, Requirement & Rationale	Testable
424	**10.15 Security Categories**	
4334	*In some organisations, only the information owners will have this privilege. In others, different roles, such as security reviewers or line managers (if such roles exist) will have these privileges.*	
2176	The ERMS must allow, but not necessarily require, security categories to be made up of one or more "sub-categories".	Y
3505	*For example, a security category may be made up of three sub-categories, as in the following fictitious example:*	
4335	• *Security Class;* • *Caveat;* • *Descriptor.*	
4598	*Each sub-category can be thought of as one dimension defining the security of information. So, in this example, any valid combination of the three sub-categories security class, caveat and descriptor can be applied to record.*	
4336	The ERMS must require controlled vocabularies to be defined and maintained by an administrative role, these vocabularies limiting the allowable values for each sub-category	Y
4337	*For example, the sub-categories might be as in the following fictitious example:*	
3506		
3507	*In this fictitious example, the sub-category "Security Class" is hierarchic (see* <ID2174>*) while the other sub-categories are not. Requirements for hierarchic sub-categories are common; these are specified below.*	
4153	*Requirements for non-hierarchic sub-categories can be complex and are specific to the sector in which they are employed; with the exception of requirements* <ID2175> *and* <ID4338> *they are not detailed here.*	
2175	The ERMS should allow specific implementations of complex or unique security rules.	N
3508	*These may be provided by suitable application program interfaces. Examples of the need for these include a need to manage records using marking conventions not covered here such as IDO (International Defence Organisation) markings, or access restrictions for medical records.*	
2174	For at least one sub-category, the ERMS must support a hierarchy of at least five levels, from unrestricted access at the lowest level to highly restricted access at the highest level.	Y
3509	*The sub-category "security class" in requirement* <ID2176> *is an example of this.*	

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

Figure <C10 ID 3506>

ID	Text, Requirement & Rationale	Testable
424	**10.15 Security Categories**	
4338	Where a sub-category and the corresponding clearances are not hierarchical, the ERMS must allow one of the following options to be selected at configuration time: • the ERMS must require a valid clearance to be entered for each new user; • the ERMS must apply a default clearance for new users. An administrative role must be able to redefine the default clearance at configuration time or any other time."	Y
4339	*In other words, the clearances must be mandatory for users.*	
4155	Where the ERMS applies a default hierarchical clearance to new users (as in <ID4338 above>) it must apply a default clearance for new users that is the lowest clearance in the hierarchy that is, the most restricted)	Y
2172	The ERMS must restrict access to records (and classes, files, sub-files and volumes depending on the selection made for <ID2178>) to those users who have a security clearance equal to, or higher than, the security category.	Y
3511	*Note that a clearance may not be sufficient to obtain access. Access to the electronic records may in addition be restricted to specified users, roles and/or groups, using features described in chapter 4.*	
2171	Where a sub-category is hierarchical, the ERMS must use one of the following modes of operation to assign a sub-category to new classes, records etc., selectable at by an administrative role at configuration time (or any later time): • the ERMS must apply a default value that is selected by an administrative role; • the ERMS must use the parent aggregation's value as a default; • the ERMS must require an administrative role to enter a value.	Y
4647	Where a sub-category is non-hierarchical, the ERMS must use one of the following modes of operation to assign a sub-category to new classes, records etc., selectable at by an administrative role at configuration time (or any later time): • the ERMS must apply a default value that is selected by an administrative role; • the ERMS must use the parent aggregation's value as a default; • the ERMS must allow but not require an administrative role to enter a value.	Y
4360	When a new hierarchical security category or subcategory is defined, the ERMS must apply a default value for all existing classes, records etc. that is the lowest value, i.e. most restricted, in the hierarchy.	Y
4361	The ERMS should allow security clearance to be allocated to a role and inherited by users. Where a security clearance is inherited from a role, the ERMS must allow a different security clearance to be applied at the individual user level.	Y
2170	If the ERMS supports security categories for both records and classes etc. (see <ID2178>), it should be capable of preventing a class, file, sub-file or volume from having a lower security category than any record within it.	Y
2169	An administrative role must be able to determine the highest security category of any record in any class, file, sub-file or volume by means of one simple enquiry.	Y
3513	*In some environments, this will be an important feature to aid manageability.*	
3518	An administrative role must be able to amend the security category of a class, file, sub-file, volume or record at any time.	Y
2168	The ERMS should support routine, periodic, scheduled, review of security categories, where a review consists of: • allowing a user (with appropriate clearance and permissions) to view specified records and their security categories; • allowing the user to change the security categories.	Y
4340	*MoReq2 does not prescribe how this is achieved.*	

ID	Text, Requirement & Rationale	Testable
424	**10.15 Security Categories**	
3519	The ERMS must automatically hold a history of security category values, in the metadata of the records, classes etc. to which they apply.	Y
4341	When a user changes the value of a security category (either during a review as in <ID2168> or otherwise), the ERMS must allow the user to enter a reason for the change, and must store the reason with the history (as in <ID3519>) as metadata.	Y
4342	The ERMS must allow users who have clearance and permissions that allow them to see a record to see the current value(s) of its security category(ies) and any history (as in <ID3519>).	Y
3522	The ERMS should support the allocation of a security category to a class, file, sub-file or volume, which is valid for a defined period of time, and should automatically downgrade the marking to the lowest level security category at the end of that period.	Y
3520	The ERMS should support the allocation of a security category to a class, file, sub-file or volume, which is valid for a defined period of time, and should automatically downgrade the marking to a lower, pre-selected, security category at the end of that period.	Y
3521	The ERMS should support notification to an administrative role of the expiry of a selected time period for which a security category has been allocated to a class, file, sub-file or volume, and allow the security marking to be reassessed and amended.	Y
4154	*For example the ERMS should send a notification at "Date of Birth + x years." This is for use in medical records or for other data protection purposes.*	
4343	The ERMS must automatically record all changes to security category and sub-category values in the audit trail.	Y
4344	The ERMS must not allow a user to apply a security category to a class, file, sub-file or volume that the user does not have access to.	Y

11 Non-Functional Requirements

ID	Text, Requirement & Rationale	Testable
1151	**11 Non-Functional Requirements**	
1152	Some of the attributes of a successful ERMS implementation cannot be defined in terms of functionality. In practice, non-functional requirements are important to success.	
3997	These non-functional requirements are often difficult to define and, and difficult to measure objectively; it is nevertheless valuable to identify them so that they can be considered, at least at a high level. Some are specific to EDRM, but several are generic to many kinds of IT system.	
1153	In addition to this chapter, users of this specification will need to consider organisational needs in relation to current technical and operational standards, and in relation to the ERMS supplier's support services including documentation, customisation, training and consultancy.	
1154	Organisations will need to add their own requirements in these areas, depending on their size and structure, physical characteristics and current technical operating environment. This section is intended as a checklist of aspects which users will need to consider when developing their specific requirements. These will need to be added to the generic requirements given in earlier sections.	
1155	Some of the Example Requirements in this chapter use angled brackets to indicate that a user of the specification needs to enter a quantified value or some other application-specific information. For example,	
1156	<*xx* minutes/hours>	

ID	Text, Requirement & Rationale	Testable
1151	**11 Non-Functional Requirements**	
1157	means that a user of the specification should enter a length of time, probably measured in minutes or hours, to suit the specific requirement.	
4055	Similarly,	
1158	<4 seconds>	
1159	means that the specification user should specify a time interval; 4 seconds is here suggested as a starting point, for consideration.	
4056	In the same way, alternative phrases are also found in angled brackets. So for example the phrase	
4059	<every day/on all weekdays/*xx* days per year>	
4058	should be taken to mean "every day, or every weekday, or on a specified number of days per year or similar" as appropriate for the organisation.	
4057	In all cases, "*xx*" may mean any number, no matter how large or small.	
4655	Because the requirements are generic, and because different organisations will have widely differing requirements and priorities, the non-functional requirements in this chapter are not tested in the MoReq2 testing framework. Organisations will need to analyse their requirements, set their priorities, and conduct their own tests in these areas.	
1160	The sections in this chapter list requirements for the following areas: • ease of use (section 11.1); • performance and scalability (section 11.2); • system availability (section 11.3); • technical standards (section 11.4); • legislative and regulatory requirements (section 11.5); • outsourcing and third party management of data (section 11.6); • preservation and technology obsolescence (section 11.7); • business processes (section 11.8).	

11.1 Ease of Use

ID	Text, Requirement & Rationale	Testable
1168	**11.1 Ease of Use**	
1170	When considering non-functional requirements in developing an ERMS specification, these must include the degree of ease of use required, and how it is to be specified. This will depend on the kinds of user for whom the system is intended, and the amount of training that is to be undertaken. Examples of requirements for ease of use are listed below.	
2436	**Example Requirement**	
4202	The ERMS must allow an administrative role to configure how much of the classification scheme a user role or group of users sees.	
4216	*For example a user or group of users, e.g. caseworkers, may be limited to viewing a single class of the classification scheme or even specific files or sub-files.*	
2457	The ERMS must provide online help throughout the entire system.	
2453	The online help in the ERMS should be context-sensitive.	
2456	The ERMS should include help on use of the classification scheme, including at a minimum *easy access to the description metadata for classes, files, sub-files and volumes.*.	

ID	Text, Requirement & Rationale	Testable
1168	**11.1 Ease of Use**	
4583	*The ERMS should include a thesaurus to assist users in selecting terms for keywords, descriptions etc.*	
2452	All error messages produced by the ERMS must be meaningful, so that users can decide how to correct the error or to cancel the process.	
3976	*Ideally, each error message will be accompanied by explanatory text and an indication of the action(s) which the user can take in response to the error.*	
2448	The ERMS user interface should be suitable for users with the widest range of needs and abilities; that is, designed according to suitable accessibility standards and guidelines, and compatible with common specialised accessibility software.	
3673	*See Appendix 7 section 3 for appropriate standards and guidelines.*	
3675	The ERMS documentation should be provided in a useful format such that users with widest range of needs and abilities have the greatest chance of using it.	
3676	*See Appendix 7 section 2 for appropriate standards and guidelines.*	
2447	The ERMS must be easy to use and intuitive throughout.	
3998	*Ease of use may be assessed by a panel of typical users.*	
2451	The ERMS user interface rules and behaviour must be consistent across all aspects of the system including windows, menus and commands. These must also be consistent with the operating system environment in which the ERMS operates.	
3977	*The rules should be consistent with other mainstream applications already installed.*	
2450	The ERMS must be able to display simultaneously multiple records and files.	
4061	The ERMS must support a graphical user interface.	
2446	The ERMS must allow users to move, re-size and modify the appearance of the windows, and to save modifications into their user profile so that they take effect automatically each time the users logs on to the ERMS.	
2440	The ERMS must allow users to customise aspects of the graphical user interface. Customisation should include, but need not be limited to the following changes: • menu and toolbar contents; • screen layout; • use of function keys; • on-screen colours, fonts and font sizes; • audible alerts.	
2445	The ERMS should allow users to select sound and volume of audio alerts, and to save modifications into their user profile.	
2444	The ERMS must allow persistent defaults for data entry where desirable. These defaults should include: • user-definable values; values same as previous item; • values derived from context, e.g. date, file reference, user identifier; as appropriate.	
4000	The ERMS must allow configurable drop down menus or "pick lists" for metadata elements.	
4001	*The content of these lists should be configurable by an administrative role.*	
2443	Frequently-executed ERMS transactions must be designed so that they can be completed with a small number of interactions (e.g. mouse clicks or keystrokes).	
2442	The ERMS should be tightly integrated with the organisation's e-mail system in order to allow users to send records and files electronically without leaving the ERMS.	

ID	Text, Requirement & Rationale	Testable
1168	**11.1 Ease of Use**	
2942	*For example the user should be able to send from the ERMS mail client. The essence of this requirement is that the user must not have to switch to the e-mail application to send the record.*	
2441	Where requirement <ID2442> is met, the ERMS should provide this by sending pointers or links to files and records rather than copies, whenever a file or record is sent to another user of the ERMS.	
3978	*There may be exceptions to this, for example, a remote user who does not have consistent access to the central repository.*	
2745	The ERMS should indicate whether an e-mail message has an attachment.	
2861	*For example, by means of an icon.*	
2439	The ERMS should support user-programmable functions.	
3979	*For example, user-definable macros.*	
2438	Where users have to enter metadata from records which are images of printed documents (e.g. scanned images), the ERMS should provide features to allow the use of optical character recognition to capture metadata from the image (zoned optical character recognition).	
4062	*For example, the user should be able to select a rectangle of the image that contains metadata such as a date or a title, then convert that image to a metadata value and insert it into the desired metadata element, all in one action.*	
2437	The ERMS should allow users to define cross-references between related records, both within the same file and in different files, allowing easy navigation between the records.	
2290	When viewing or working with a record or aggregation (e.g. class, file, sub-file or volume) of records, whether as the result of a search or not, a user should be able to use ERMS features to find information about the next-higher level of aggregation of records easily and without leaving or closing the record.	
3766	*For example, when reading a record, the user should be able to find out what class, file, sub-file or volume it is in; if viewing file metadata, the user should be able to find out information about the class in which it is located.*	
4063	The ERMS should allow a user who has access to a file or record to check whether another specified user, group or role has access to it.	
4064	*This is to permit users to specify a user, group or role explicitly. Thus a user can enquire about the rights of another user, in the context of a record or file, without needing to know that user's group or role memberships.*	
4065	The ERMS should allow a user to mitigate the risk arising from an error in filing a record by allowing users to place a temporary lock on a record or file with a single click. This temporary lock should bar access to that file or record to all users save for administrative roles; and the ERMS should automatically inform an administrative role that the temporary lock has been applied, allowing the administrative role (and nobody else) to remove the temporary lock.	
4066	*This is to allow users to correct an error - such as accidentally placing a sensitive record into an unsecured file, perhaps as part of a "drag and drop" operation. Because users are not able to delete, remove or change records, this requires administrative action.*	
4067	Users should be able to copy records from the ERMS into other working environments, such as a "desktop" folder, using "drag and drop", so long as the record remains unchanged in the ERMS.	
4068	*When a record is dropped into any other environment, it will be acceptable for it to lose its metadata (on the basis that most other environments do not support the MoReq2 metadata model).*	

ID	Text, Requirement & Rationale	Testable
1168	**11.1 Ease of Use**	
4070	The ERMS should provide help which provides visual guidance.	
4071	*For example, including partial screen shots and/or animations showing users how to use system features.*	
4072	The ERMS should allow users to mark areas of the help system as "favourite" areas or similar, so that they can find them easily on later occasions.	
2820	A user working with a file must be able to discover easily and quickly the keywords associated with that file.	
2826	*It must be possible to discover the keywords without having to leave the file, in a way that allows work with the file to be continued without interruption.*	

11.2 Performance and Scalability

ID	Text, Requirement & Rationale	Testable
1212	**11.2 Performance and Scalability**	
1213	Users of this specification should consider the extent to which the ERMS provides rapid response times (in line with user expectations), and is capable of serving the size of user population for which it is intended. Some considerations and example requirements are given below.	
1214	The response times experienced by users will depend on factors outside the ERMS, including: • network bandwidth; • network utilisation; • network latency; • configuration and utilisation of various server resources.	
1218	This specification cannot address such external factors, other than to point out that they must not be ignored. Usually, tests in the live environment are needed to obtain a reliable view of performance.	
1219	Accordingly, these requirements should be interpreted with a standardised understanding of "response time". This standardised understanding will vary from environment to environment, depending on the status of the infrastructure.	
4038	For example, if the ERMS is being specified for an existing infrastructure, it may be appropriate to specify response time in terms of the time between receipt of a keystroke at the server, and the sending of the response; alternatively, if the ERMS is being specified for a new network it may be more appropriate to specify response time in terms of the time between keying a request at the workstation and receiving the response at the workstation.	
4039	Specific requirements for offline and remote working are covered in chapter <10.13> and these example requirements will need to be further modified in these environments.	
4040	The ERMS must be able to perform all functions and operate consistently to meet business and user needs as defined in the example requirements below.	
2458	**Example Requirement**	

ID	Text, Requirement & Rationale	Testable
1212	**11.2 Performance and Scalability**	
2466	The ERMS must provide adequate response times to meet business needs for commonly performed functions under standard conditions, for example: • <100%> of the total anticipated user population logged on and active; • <100%> of the anticipated total volume of documents managed by the system; • users performing a typical mix of transaction types at various rates; with consistency of performance over at least ten transaction attempts.	
2465	The ERMS must be able to return the results of a simple search (the hit list) within <3 seconds> and of a complex search (combining four terms) within <10 seconds> regardless of the storage capacity or number of files and records on the system.	
3980	*In this context, performing a search means returning a hit list (see section <x.x>). It does not include retrieving the records themselves.*	
2464	The ERMS must be able to retrieve and display within <4 seconds> the first page of a record which has been accessed within the previous <*xx*> months, regardless of storage capacity or number of files/records on the system.	
4584	*This requirement, and the next, apply only to documents that can be presented in the form of pages. If the document are unusually large, it may be necessary to extend the acceptable response time.*	
4076	*The inclusion of "*within the previous <*xx*> months*" implies the use of a staged or "hierarchical" physical storage mechanism. See also the next requirement.*	
3981	*This requirement is intended to allow for rapid retrieval of frequently-used records, on the understanding that frequency of use is typically correlated with recent use. The timescale is to be inserted by the organisation, based on an evaluation of the time after which the heavy usage of records decreases.*	
2463	The ERMS must be able to retrieve and display within <20 seconds> the first page of a record which has not been accessed within the previous <*xx*> months, regardless of storage capacity or number of files/records on the system.	
3982	*This requirement is intended to allow for cases where a form of hierarchical storage management is used, where records used infrequently are stored on slower media than more active records, or stored near-line. The timescale is to be inserted by the organisation, based on an evaluation of the time after which the heavy usage of records decreases.*	
4077	*For both this and the preceding requirement, if all the electronic records are stored using a single physical mechanism (i.e. without staged or hierarchic storage) then the phrase "*within the previous <*xx*> months*" is irrelevant and should be deleted.*	
2462	The ERMS must allow a single implementation of the system to have an electronic record store of at least <*xx* gigabytes/terabytes/petabytes> or <*xx* thousand/million/billion> records, and to serve at least <*xx* hundred/thousand> users simultaneously with the performance levels specified in this section.	
3983	*Estimates of storage requirements and record and user population to be inserted by the organisation. Note that in large organisations, large volumes of records may accumulate - in some cases this will extend into the billions of records.*	
4559	The ERMS must provide the performance levels specified in this section with volumes up to At least: • <*xx*> classes; • <*xx*> files per class; • <*xx*> volumes per file; • <*xx*> records per volume.	

ID	Text, Requirement & Rationale	Testable
1212	**11.2 Performance and Scalability**	
4560	*These are indicative metrics only. Organisations should consider whether other similar metrics apply to their circumstances.*	
2461	It must be possible to expand the ERMS, in a controlled manner, to meet organisational growth up to at least <*xx* hundred /thousand> users while providing continuity of service.	
4561	*The intention of this requirement is that expansion should be possible with only "routine" upgrades that do not result in major interruptions in availability.*	
2460	The ERMS must support the above performance level, including routine maintenance of: • roles, users and user groups; • security categories; • access profiles; • classification schemes; • databases; • retention and disposition schedules; in the face of the anticipated levels of organisational change, without imposing undue systems down time or account administration overheads (see also chapter 9).	
3984	*In cases where performance requirements are strict, it may be necessary to quantify the anticipated levels of organisational change.*	
2459	The ERMS must be scaleable and must be able to be used in small or large organisations, with varying numbers of differently-sized organisational units and across different geographical locations.	

11.3 System Availability

ID	Text, Requirement & Rationale	Testable
1240	**11.3 System Availability**	
1241	In many organisations the introduction of an ERMS and EDMS together will increase users' dependence on the IT network to the extent that they will be unable to continue working if the ERMS and EDMS become unavailable.	
4025	Accordingly, users of this specification who are procuring a system should make every effort to identify user requirements for availability, and then to specify these for the procurement. Example requirements for availability are given below.	
2467	**Example Requirement**	
2472	The ERMS must be available to users: from <*xx*:00> to <*xx*:00> <every day/on all weekdays/*xx* days per year>.	
2471	Planned downtime for the ERMS must not exceed <*xx*> hours per <rolling three month period>.	
3985	*The definition of "downtime" may depend on the infrastructure and architecture. For example, in some environments, a failure caused by server hardware will be considered as a failure of the ERMS; in other environments such a breakdown will be considered as a different kind of failure, not attributable to the ERMS.*	
4003	*A suitable definition needs to be agreed; as a starting point the following is proposed: "The ERMS is considered to be down if more than <xx%> of users are unable to perform any normal ERMS function and if this failure is attributed to any component of the ERMS other than the user's workstation."*	
2470	Unplanned downtime for the ERMS must not exceed <*xx* hours/minutes> per <rolling three month period>.	

ID	Text, Requirement & Rationale	Testable
1240	**11.3 System Availability**	
2469	The number of incidents of unplanned downtime for the ERMS must not exceed <*xx*> per <rolling three month period>.	
2468	In the event of any software or hardware failure, it must be possible to restore the ERMS to a known state (no older than <the previous day's backup>) within no more than <*xx*> hours of working hardware being available.	

11.4 Technical Standards

ID	Text, Requirement & Rationale	Testable
1255	**11.4 Technical Standards**	
1256	The ERMS should comply with relevant de facto and de jure standards. Where possible, it is desirable that the ERMS should make use of open rather than proprietary interfaces.	
1257	Users of this specification may need to specify requirements for standards covering: • hardware environment (for server platforms and workstation environments); • operating system environment (for server platforms and workstation environments); • workstation (client) software architecture; • user interface; • relational database and interface; • network protocol and network operating system; • interchange standards; • application program interface and developer kits.	
1266	When using this specification for procurement, it will be necessary to add further details of the technical environment, including all ERMS interfaces (e.g. legacy systems, office systems) and any plans for change.	
1267	Additionally, users of this specification will need to consider their individual requirements for standards:	
4005	*See Appendix 7.1 for a definitive list of the standards used in this specification.*	
2473	**Example Requirement**	
2484	If a monolingual thesaurus is implemented with the ERMS, it should comply with standard ISO 2788, Guidelines for the establishment and development of monolingual thesauri.	
2483	If a multilingual thesaurus is implemented with the ERMS, it should comply with standard ISO 5964, Guidelines for the establishment and development of multilingual thesauri.	
2481	The ERMS must support the storage of records using file formats and encoding which are either de jure standards or which are fully documented.	
4004	*Users may wish to specify file format and encoding requirements for their organisation.*	
2478	The ERMS should store all dates in a format compliant with ISO 8601, Data elements and interchange formats - Information interchange - Representation of dates and times.	
2477	The ERMS should store all country names in a format compliant with ISO 3166, Codes for the representation of names of countries.	
2476	The ERMS should store all language names in a format compliant with ISO 639, Codes for the representation of names of languages.	
2474	If the ERMS is to manage records in multiple languages or using non-English characters, it should be capable of handling ISO 10646 encoding (Unicode).	

11.5 Legislative and Regulatory Requirements

ID	Text, Requirement & Rationale	Testable
1293	**11.5 Legislative and Regulatory Requirements**	
1294	The ERMS must conform to legislative and regulatory requirements, which typically vary from region to region and between industries.	
1295	MoReq2 does not address the need to maintain physical records. Such a need may or may not exist, according to the legislative and regulatory environment; where there is such a need, care needs to be taken to preserve integrity and usability of electronic and physical records taken as a whole. These issues should be addressed by appropriate organisational policies.	
1296	The following requirements will require localisation, in a "chapter zero".	
4585	In addition, users of MoReq2 will need to consider requirements that are specific to their industry, market sector, etc.	
2485	**Example Requirement**	
2489	The ERMS must conform to locally-applicable standards for legal admissibility and evidential weight of electronic records.	
2488	The ERMS must comply with locally-applicable records management legislation.	
2487	The ERMS must not include any features which are incompatible with locally-applicable data protection, freedom of information or other legislation.	
2486	The ERMS must comply with any locally-applicable European, national or local regulatory requirements, guidelines or codes of practice for the industry, business function or sector.	

11.6 Outsourcing and Third Party Management of Data

ID	Text, Requirement & Rationale	Testable
1310	**11.6 Outsourcing and Third Party Management of Data**	
1311	Many organisations use external service providers to store and manage records. In some cases, these are records that are no longer active (or have low recall requirements) but which need to be retained for a legislative period demanded by legal/government stipulation, industry regulators or for long term preservation.	
1312	Other organisations use Application Service Providers (ASPs) to manage active records as well as those that have been archived. Organisations send their documents or records - invoices, customer correspondence, mortgage application documents etc. - to be indexed and stored by the ASP. The documents are then available for retrieval and presentation by the organisation's staff over the internet or through a wide area network.	
1313	The management of electronic records by a third party requires that the contract with the service provider has clearly defined procedures and controls in place in order to meet regulatory requirements, adhere to best practice for legal admissibility of electronic records, and meet the business demands of the client for access and availability.	
1314	The contract will need to include provisions that: • the service provider's management must be to a standard at least as good as that of the client's management of its records internally; • the client will be able to recover the records from the service provider in the future, and still be able to continue the management of the records to the organisation's standards and meet legal admissibility requirements.	
1317	This sub-section draws heavily on ISO 15801 (see Appendix 1).	
2491	**Requirement**	

ID	Text, Requirement & Rationale	Testable
1310	**11.6 Outsourcing and Third Party Management of Data**	
2505	A contract or Service Level Agreement (SLA) must be agreed with the service provider detailing the services that are to be used.	
4008	*An SLA is a formal negotiated agreement between the client and the service provider. It records the agreed position regarding services, priorities, responsibilities, etc.*	
2504	Details of the procedures for the transfer of records from the client to the service provider, and from the service provider to the client, must be documented.	
3990	*This may use communication links between the sites to transfer files and records automatically on a daily or regular basis. The client must be satisfied that the link between the two sites is secure and the protocols are in place to check all records are received, and reports produced listing any discrepancy.*	
2503	The service provider must be able to provide the client with copies of the audit trail of the processes for logging and storing of the records/files.	
2502	The service provider must demonstrate that the files/records and metadata stored can be easily transferred back to the client's ERMS without any loss of structure, context, metadata or content of the records.	
4006	The service provider must have procedures in place to allow the client to transfer individual files and records.	
2501	The service provider must be able to provide ready access to the managed records by the client. The service provider must either deliver a presentation of the record, or the original record to the client to a contracted agreed time and price.	
2500	The service provider should be able to provide the client with the ability to request, view and print records and or files from the client's office.	
3991	*This can be achieved, for example, by a network connection.*	
2499	The service provider should be able to provide the client with the ability to request on-line the downloading or transmitting of records and or files between the client's ERMS and service provider's storage facility.	
2498	The client should be able to request reports on the records held by the service provider and details of retention and disposition schedules etc. This facility should be provided on-line from the client's offices.	
2497	Services specified in <ID2500>, <ID 2499> and <ID2498> should: • have contracted response and/or turnaround times; • operate in a secure environment.	
2496	The client should check that the proposed location of the work is acceptable and that the location meets security criteria appropriate to the client's needs.	
2495	The client should check that the proposed procedures and storage management processes involve no greater risk to the records than the client's own procedures.	
3992	*The service provider will need to demonstrate that all the client's records are backed up and in the event of system failure they can be recovered to a contracted timescale.*	
2494	The client should check that the service provider will provide suitable operational staff where the security of the records is important.	
3993	*It is an advantage if all employees of the service provider sign a confidentiality agreement as part of their conditions of employment.*	
2493	Each shipment of records to/from the client and the service provider should be accompanied by a control document stating the identity and number of records and files.	
2492	Third parties providing transportation services should be organisations that meet the quality and reliability criteria of the client.	

11.7 Long Term Preservation and Technology Obsolescence

Note to reviewers: This section has not been fully revised. A new draft will be published shortly.

ID	Text, Requirement & Rationale	Testable
1349	**11.7 Long Term Preservation and Technology Obsolescence**	
1350	This section addresses long term preservation. "Long term" is not defined precisely; but it is understood here to mean "for a period of more than ten years or so". In any organisation, the retention period of any particular record should be determined by legislation and business needs. In some environments, this will mean several decades; in some archives it may extend to centuries. In either case, the time period is sufficiently long that approaches used routinely for shorter periods cannot be assumed to be appropriate.	
1351	Electronic records held for the long term face risks from three directions: • media degradation; • hardware obsolescence; • format obsolescence.	
1355	These are discussed below. The discussions are followed by specific requirements. Users of this specification should note, however, that detailed requirements for all aspects of this issue are not provided; each organisation should develop and implement a strategy for the long-term preservation of its electronic records, much as is often the case for paper-based records.	
1356	In the discussion which follows, preservation of records includes the preservation of all metadata and audit trail information which accompanies them.	
1357	**Media Degradation**	
1358	The risk from media degradation arises because all digital storage media have a limited lifetime. The lifetime varies from media to media, and varies also according to storage conditions (temperature, humidity and rates of change). As media reach, or exceed, their expected lifetime, the likelihood of read errors (that is, bits read incorrectly) increases dramatically. Most storage hardware has automatic error correction built into it; this can cope with a certain level of bit errors, effectively compensating for them. But eventually, the read errors become so numerous that the automatic error correction cannot cope; at this stage, records become irretrievably corrupt. The effect of this corruption depends on many factors, but can lead to individual records or whole discs, tapes etc. becoming unreadable.	
1359	The following precautions can be taken to avoid loss of information due to media degradation: • ensure all media is stored, used and handled in suitable environmental conditions. As a general rule, the cleaner, cooler, dryer and more stable the environment, the longer the expected life. However, for specific media, the manufacturer's specifications must be followed (e.g. the environment must not be colder than a certain temperature; the media must, or must not, be periodically cleaned); • routinely replace media (by copying information from them to fresh media) before the expected end of life; • keep several copies of each record, and systematically compare copies according to a schedule; then replace any copy of a record which shows an unrecoverable error, and replace any piece of media which shows an unrecoverable error. This approach is typically used in specialist long-term data archives; it requires automated systems and retrieval hardware, further description of which are beyond the scope of this specification.	
1363	**Hardware Obsolescence**	

ID	Text, Requirement & Rationale	Testable
1349	**11.7 Long Term Preservation and Technology Obsolescence**	
1364	Storage peripherals - tape drives, disc drives - have a limited life expectancy. As they exceed this life, they typically require more maintenance, while at the same time becoming expensive to maintain and repair; eventually they become unrepairable for practical purposes. In some cases, sharing agreements can be reached with other users of similar or compatible equipment; but this is not sustainable indefinitely. At some point, information stored on obsolete devices will be lost permanently if the device fails unless it has been copied onto other media.	
1365	The same problem arises with the computers which manage the applications and storage.	
1366	Clearly the strategy to avoid this risk is to monitor the status of the hardware, and to migrate the information to new, current media before obsolescence puts the information at risk. In all cases, media and hardware should be chosen which have a good life expectancy; in other words, popular or "market leading" may be a better choice than new and state-of-the-art.	
1367	**Format Obsolescence**	
1368	Format obsolescence presents the most difficult problem for any period longer than a handful of decades.	
1369	The problem arises because the many software components involved in the processing "chain" between media and rendered information are constantly evolving. The components include: • encoding standards; • file formats; • application software; • database and other utility software; • operating system software.	
1375	Their evolution is rapid, and different components evolve in different ways, at different rates. Some evolution retains compatibility with prior formats. However, some evolution does not retain compatibility - and this is especially true over periods longer than a handful of decades. It is not possible to avoid the evolution by "freezing" the configuration, because of the need to migrate to current hardware, as described above; new hardware frequently requires new software drivers, which in turn require a new operating system, and so on.	
1376	Currently, the following techniques are recognised: • migration (converting information to new formats which can be accessed by current hardware and software); • emulation (moving the information to new hardware but with a additional software component which emulates the old hardware, thus allowing execution of the old application software); • technology preservation (continual maintenance of the original hardware; not practical in the long term); • encapsulation of data and software (a theoretical approach which is involves packaging together records, metadata, ERMS and other software in standard software "wrapper").	
1381	Although much research work is under way to minimise the risk, there is at time of writing no simple, generic method which will guarantee long term access to electronic records. The consensus is that migration and/or emulation are likely to be the safest options; in practice, both will require attention to preservation metadata - see below.	

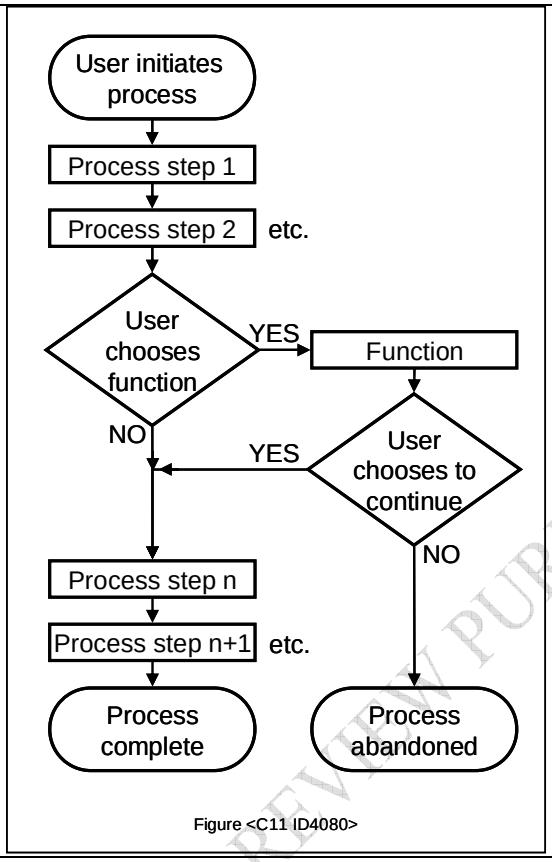
ID	Text, Requirement & Rationale	Testable
1349	**11.7 Long Term Preservation and Technology Obsolescence**	
1382	However, large-scale migrations are rarely free of problems; they can result in the loss of individual items, and they sometimes result in loss of functionality, detail, or some other characteristic.	
1383	Likewise, large-scale, long-term emulation is not well-understood. It also has risks of loss of functionality and other characteristics.	
1384	The difficulties are compounded by the prospect of repeated migrations or emulations. Nobody can predict the nature of the migrations or emulations which may be required; and nobody can predict the consequences of repeated migrations or of several "layers" of emulation.	
1385	The most appropriate strategy is to hold information only in widely-accepted, stable, open formats (i.e. formats which are comprehensively documented in publicly-available specifications) which have a long expected life. As with hardware, this suggests "market leading" rather than unproven or state-of-the-art; and it suggests proprietary formats should be avoided where their specifications are not publicly available. Examples of suitable formats include XML files and PDF/A. There is also an implication that the organisation will need some expertise when selecting formats.	
1386	The volatility of the multimedia market, and of the proprietary formats it uses, makes multimedia an area of particular concern.	
1387	As this problem requires an organisation-specific response, more detailed discussion at the generic level of this specification would not be helpful. However, it is appropriate to point out that each approach involves expense - in hardware, software, data preparation and conversion, and management - and yet none will preserve access unless a strategy for long-term preservation is implemented before accessibility becomes problematic. In other words, long-term preservation requires the preventive expenditure of amounts which may grow to be large; this is similar in concept to the preservation of paper archives, save that in some cases the expenditure will be larger. Where long term preservation is required, it is therefore essential that senior management is committed to the ongoing effort and expense required to safeguard access. Further sources of information are given in Appendix 7 part 4.	
1388	**Preservation Metadata**	
1389	It is essential that preservation metadata be stored with the records when long term storage is needed. This metadata provides information beyond the scope of the metadata outlined in this specification, such as information about the technical environment, about the software used to create a record and about software needed to present a record - and all its components. Where the preservation period is unlimited, the number of metadata elements required becomes large. Several research projects in Europe, North America and Australia have developed metadata frameworks. The complex nature of the preservation metadata has led to the development of the ISO 14721 OAIS Open Archive System reference model (see Appendix 7), which can be used to structure metadata for preservation purposes.	
1390	**Specific Requirements**	
1391	The requirements in this section are proposed as a minimum technical requirement where long-term storage is envisaged. However, as indicated above, management commitment is equally important.	
2506	**Requirement**	
2513	The ERMS storage media must be used and stored in environments which are compatible with desired/expected lifespan, and which are within the tolerance of the media manufacturer's specification.	

ID	Text, Requirement & Rationale	Testable
1349	**11.7 Long Term Preservation and Technology Obsolescence**	
4029	The ERMS must support the monitoring and replacement of storage media to guard against media degradation.	
2512	The ERMS should include features for the automated periodic comparison of copies of information, and the replacement of any copy found to be faulty, to guard against media degradation.	
2511	The ERMS must allow the bulk conversion of records (together with their metadata and audit trail information) to new media and/or systems in line with the standards relevant for their format(s).	
2510	The ERMS supplier must have a system upgrade programme in place to ensure that the existing information can continue to be accessed without changes to the content.	
4009	Any system modifications that have been made to the ERMS for organisational requirements must remain in place following a system upgrade.	
4586	The ERMS should be able to report on file formats held, for both records and their components.	
4587	*For example, the ERMS should be able to produce lists of record and components in specified file formats. This facility would be used in conjunction with a software intelligence, or preservation monitoring, function that aims to identify file formats that are at risk of obsolescence.*	
4026	The ERMS should be able to render (see Glossary) records from their original format to a any specified long-term preservation file format(s) at the time of capture, on a subsequent occasion, or on export.	
4027	*It is acceptable for the rendering process to be undertaken by a program external to the ERMS so long as the context and links are maintained at all times.*	
4588	Wherever possible without compromising the integrity of the records, the ERMS should be able to render components from their original format to a any specified long-term preservation file format(s) at the time of capture, on a subsequent occasion, or on export.	
4589	*It is acceptable for the rendering process to be undertaken by a program external to the ERMS so long as the context and links are maintained at all times.*	
4590	*Where components are migrated, it is essential that the integrity of the records that they form is maintained. The feasibility of this approach generally will depend on the capabilities of both the migration process and of the software application or viewer used to present the records. For example, if the records are web pages that include(say) GIF image files, it would be acceptable to migrate the GIF images only if the following are all true:* • *the GIF components are migrated to a file format that can be presented by the application used to access the web pages; in this example, it is likely that JPEG would be suitable;* • *the references to the GIF images in the web pages are amended as part of the migration process so that they refer instead to the new JPEG images;* • *the original components (the unamended web pages and unmigrated GIF components are retained alongside the new components.* *This example is chosen solely for illustration and does no indicate that there is any reason to migrate GIF images at the time of writing.*	
4591	*In many cases it will be difficult or unfeasible to achieve this, and alternative preservation approaches will be needed.*	
4028	The ERMS must be able to maintain links between different renditions of the same records and enable disposition actions to be carried out on them simultaneously.	

ID	Text, Requirement & Rationale	Testable
1349	**11.7 Long Term Preservation and Technology Obsolescence**	
4592	When a record has been rendered into a preservation file format, the ERMS must provide suitable facilities to retrieve the original format and/or renditions, as appropriate.	
4593	The ERMS should be able to export records and their metadata in the form of a Dissemination Information Packages as defined by the OAIS standard, ISO 12654, (see Appendix 7.1).	
4030	The ERMS should hold at a minimum the following metadata items for a rendered record: • the original format; • date of conversion.	
2508	If the ERMS uses any proprietary encoding or storage or database structures, these must be fully documented, with the documentation being available to administrative roles.	
3995	*This implies it may not be sufficient for the supplier to retain a copy of the documentation; in the timescale being considered, the stability of the supplier is not certain. It may therefore be desirable for a copy of this documentation to be lodged with the user organisation or with a neutral third party.*	
2514	The ERMS should be able to manage a range of preservation metadata elements for the records and their component parts.	
3996	*See <Appendix 9>.*	

11.8 Business Processes

ID	Text, Requirement & Rationale	Testable
4049	**11.8 Business Processes**	
4050	Experience has shown that the success of ERMS installations depends, among other factors, on how easy or difficult it is to perform functions. If an ERMS contains all the features needed for records management, document management etc., an implementation will only succeed if users find it easy to use; if users find it difficult to use, it will be rejected despite its capabilities.	
4051	In recognition of this finding, this section describes requirements intended to promote ease of use. Accordingly, most of the requirements are desirable rather than mandatory. The requirements may be met by workflow software that is integrated with the ERMS, so long as they are fully configured and working.	
4078	Some of the requirements below call for the ability to perform a specified function "…as an integrated part of a process". In all cases, this means that a user who is performing a process should: • have the option of performing the process, or of not performing it; • be able to initiate the function easily, preferably with a single click, and without needing to re-enter information that has already been entered; • be able to choose, at the end of the function, either to cancel the original process or to return to it at the same point and with the same status as before the function was initiated (i.e. without needing to re-enter information that has already been entered).	
4079	This is illustrated in diagram <C11 ID4080> below.	

ID	Text, Requirement & Rationale	Testable
4049	**11.8 Business Processes**	
4080	 Figure <C11 ID4080>	
4597	All of the following requirements are to be interpreted as being dependent on user access rights.	
4081	**Requirement**	
4082	The ERMS should allow a user who is allowed to change the security category of any record, file or class to check its existing category and permissions as an integrated part of the process of changing it.	Y
4083	When a user is warned about the lowering of a security category of a record (see chapter 9 <ID2351>) the user should be able to examine the record and/or its metadata as an integrated part of the process.	Y
4084	Whenever a new file or sub-file or volume is created, and where a physical container exists for it, the ERMS should allow the user to print an appropriate label for the physical container, as an integrated part of the process.	Y
4594	*This enables a label to be produced containing essential metadata which can then be attached to the physical entity. This could include, but is not limited to, such metadata as:* • *Title;* • *Identifier - System;* • *Classification Code;* • *Date of Opening;* • *Security Category (if used);* • *Normal storage location.*	
4085	Whenever a user deleting any information receives a warning about existing links (see section 9.3) the user should be able to examine the links and the linked information and/or its metadata as an integral part of the process.	Y

ID	Text, Requirement & Rationale	Testable
4049	**11.8 Business Processes**	
4086	The ERMS should allow a user who is redacting a record, to achieve the following in a single integrated process: • redact the record; • create an extract; • decide where in the classification scheme the extract should be filed, and declare it as a record; • link the extract to the original record; • link the original record to the extract.	Y
4087	When a user is declaring a record, the ERMS should allow the user to check whether a document has already been declared as a record, as an integrated part of the process.	Y
4088	*This should apply to any kind of document.*	
4089	The ERMS should warn a user who is declaring a document as a record if that document has already been declared, informing the user of where it is allocated (class, file etc.) and giving the user the option to continue with or abandon the declaration.	Y
4090	When a user is declaring a record, the ERMS should allow the user to: • browse the classification scheme (to find the desired class, file etc); • look at the metadata (permissions, keywords, descriptions etc) of any classes and files; • before the declaration is completed, as an integrated part of the process.	Y
4091	When a user is declaring a record that has a security category higher than the default, the ERMS should allow the user to check who (which other users, groups, roles) has access to the record before the declaration is completed, as an integrated part of the process.	Y
4596	*The intent of this requirement is to allow a user to check who will be able to see a record before it is irrevocably stored. For example, a manager may wish to capture a sensitive record, without being sure which of her staff has been granted access to the security sub-category that she intends to use; this requirement allows her to ensure that she chooses the correct sub-category. Requirement <ID 4065 in section 11.1> is closely related.*	
4092	Whenever a user sees any class, file, record etc. on screen, as the result of a search, while browsing the classification scheme or in any other context, the user should be able to perform any valid action on it directly, without needing to navigate to another part of the ERMS, including at least: • opening it; • determining its parents in the classification scheme; • viewing its metadata or audit trail; • viewing and following its links; • sending it by e-mail; • changing its security category; • viewing users and roles allowed access to it; • printing (or presenting) it; • redacting it; • relocating or deleting it.	Y
4093	The ERMS should allow a user to change the security category of any record, file or class, including the updating of all affected metadata element values, in a single process.	Y

12 Metadata Requirements

ID	Text, Requirement & Rationale	Testable
1417	**12 Metadata Requirements**	
1418	This chapter presents functional requirements for managing metadata. The MoReq2 metadata "model" is presented in Appendix 9.	
3371	Metadata includes, in the context of this specification, indexing information and other data needed for effective records management, such as access restriction information. A formal definition is given in the Glossary. A more detailed explanation of the role of metadata in records management is found in ISO 23081 (see Appendix 7.1).	

12.1 Principles

ID	Text, Requirement & Rationale	Testable
1420	**12.1 Principles**	
1422	**Scope**	
1423	It is not possible to define all the metadata requirements for all possible kinds of ERMS implementation. Different kinds of organisations and applications have particular needs and traditions which vary enormously. For example, some organisations will need indexing, which is focussed on account names and transaction dates, while others will need strict hierarchical numbering; some will need volumes, which relate to financial years, while others will not; some will need access controls for security reasons, others for intellectual property reasons, and so on.	
3376	This chapter of MoReq2 therefore suggests minimum requirements which are intended as the starting point for customisation and expansion. These minimum requirements are closely related to lists of specific metadata "elements" which the ERMS must be able to capture and process. These elements make up the MoReq2 metadata model in Appendix 9.	

12.2 General Metadata Requirements

ID	Text, Requirement & Rationale	Testable
3384	**12.2 General Metadata Requirements**	
2539	The ERMS must not present any practical limitation on the number of metadata elements allowed for each entity (e.g. class, file, sub-file, volume, record).	P
3385	*The definition of "practical limitation" will vary according to the application. For example, small organisations with a small classification scheme may not need as many metadata elements as large organisations with a complex classification scheme.*	
2538	Where the contents of a metadata element can be related to the functional behaviour of the ERMS, then the ERMS must use the contents of that element to determine the functionality.	P
3386	*For example, where the ERMS stores file opening date metadata, it must populate that metadata automatically whenever a file is opened rather than requiring a user to populate it. Note that this is a general requirement which stretches across many metadata elements. MoReq2 does not attempt to identify all cases in which this is relevant.*	
2537	The ERMS must allow different sets of metadata elements to be defined for different record types at configuration time.	Y

ID	Text, Requirement & Rationale	Testable
3384	**12.2 General Metadata Requirements**	
3387	*For example:* • *invoices may need account number metadata;* • *correspondence needs multi-value recipient metadata elements;* • *records which are scanned images will need metadata relating the scanning and indexing processes.*	
2536	The ERMS must allow an administrative role to define at configuration time whether each metadata element is mandatory or optional.	Y
2540	The ERMS must support at least the following metadata element formats: • alphabetic; • alphanumeric; • numeric; • date; • logical (i.e. YES/NO, TRUE/FALSE).	Y
2535	The ERMS should support metadata element formats, definable by an administrative role, which consist of combinations of the formats in <ID 2540>.	Y
3388	*For example, a case might have a reference number in the format nnnnn/aa-n.*	
2534	The ERMS must support date formats defined in ISO 8601 for all dates.	Y
2533	At time of configuration, the ERMS should allow definition of the source of data for each metadata element.	Y
3389	*Possible sources are described in requirements* <ID2532>, <ID2531>, <ID2530>, <ID2529>.	
2531	The ERMS must allow an administrative role to specify which metadata element values are to be entered and maintained by manual entry or from selection from a controlled vocabulary.	Y
2530	The ERMS should allow for the values of metadata elements to be inherited automatically by default from the next higher level in the classification scheme hierarchy.	Y
3391	*For example, for a volume, the value of some of the metadata elements must be inherited from its parent sub-file; and for a record, the value of some metadata may be inherited from the volume into which it is stored.*	
2529	The ERMS should allow values of metadata to be obtained from lookup tables or from calls to other software applications.	Y
3392	*For example, the ERMS might provide name and post code to an addressing application which then returns a street name to be used as metadata.*	
4599	Where the metadata element is populated by lookup tables, if the selection of a value excludes other values in subsequent lookup tables, this should reflected in the values available in those subsequent tables.	Y
2521	The ERMS should be able to acquire metadata values from: • a document-creating software application (see <ID2833>); • operating system; • network software; • the user at the time of capture or declaration; • rules defined at configuration time for generation of metadata by the ERMS at the time of declaration.	Y

ID	Text, Requirement & Rationale	Testable
3384	**12.2 General Metadata Requirements**	
2528	The ERMS must validate metadata when it is entered by users, and when it is imported. The validation must use at least the following mechanisms: • Format of the element contents; • Range of values; • Validation against a list of values maintained by an administrative role.	Y
3393	*An example of format validation is that the contents are all numeric, or are in a date format (consistent with <ID2540>). An example of range format validation is that the contents fall in the range between 1 January 1999 and 31 December 2001. An example of validation against a list of values is verifying that an export destination is present on a list.*	
2527	The ERMS must be capable of validating metadata using calls to another application (e.g. to a personnel system to check whether a personnel number has been assigned, or to a post code database system) or using an internal look-up table.	Y
2541	For metadata element values that are entered manually, the ERMS must support persistent default values which are user-definable.	Y
3394	*A persistent default appears as the default in the data entry field for each item in succession until it is changed by a user. Once changed, the new value remains, i.e. becomes persistent.*	
2526	The ERMS should allow configuration such that any metadata element value can be used as a search field in a free text search.	Y
2525	Where a metadata element value is stored in date format, the ERMS should allow searches which recognise the value of the date.	Y
3396	*For example, the ERMS should support searches in a date range. It is not sufficient for the date to be stored as a text field.*	
2524	Where a metadata element value is stored in numeric format, the ERMS should allow searches which recognise the value of the number.	Y
2523	The ERMS must allow administrative roles to restrict the ability to make changes to metadata values as defined in the access control model (section <13.4>).	Y
2522	The ERMS must allow reconfiguration of the ERMS metadata model by an administrative role, and must record such in the audit trail.	P
3397	*For example, it may be necessary to add a new data element such as "Department Identifier" to some document types following an organisational change.*	
2520	The ERMS must allow metadata elements to be configured at configuration time such that values generated from other application packages, the operating system or the ERMS (for example, e-mail transmission data) cannot be modified by users once they have been captured.	Y
2519	The ERMS must allow metadata elements to be configured at configuration time such that their values cannot be modified by users once they have been captured.	Y

13 Reference model

13.1 Glossary

ID	Text
1779	**13.1 Glossary**
1780	This glossary defines key terms used in the MoReq2 Specification (i.e. in the requirements as well as in the reference model).

ID	Text
1779	**13.1 Glossary**
1781	Some significant definitions are taken from, or closely adapted from, glossaries presented in reference publications listed in Appendix 1; these sources are acknowledged below each definition.
1782	Terms defined within this glossary are shown in *italics*.
3245	**administrative role**
3246	A set of functional permissions allocated to *users* allowed to perform administrative actions.
3247	Note: In MoReq2 this term is used also to specify the people with these permissions.
1783	**administrator**
1784	A role responsible for the day to day operation of the corporate records management policy within the organisation.
1785	Note: this represents a simplification. Especially in large organisations, the tasks attributed in this specification to Administrators may be divided between several roles, with titles such as Records Manager, Records Officer, Archivist etc.
4606	**aggregation**
4607	A class, file, sub-file or volume.
1786	**audit trail**
1787	Information about transactions or other activities which have affected or changed entities (e.g. *metadata* elements), held in sufficient detail to allow the reconstruction of a previous activity.
1788	Note: an audit trail generally consists of one or more lists or a database which can be viewed in that form. The lists can be generated by a computer system (for computer system transactions) or manually (usually for manual activities); but the former are the focus of this specification.
1789	**authenticity**
1790	(in the context of records management only) The quality of being genuine.
1791	Source: Adapted and abbreviated from the definition of "record authenticity" in the UBC-MAS Glossary (Appendix 1 reference [8]).
4600	An authentic record is one that can be proven – "a) to be what it purports to be, - b) to have been created or sent by the person purported to have created or sent it, and - c) to have been created or sent at the time purported." - Source: ISO 15489.
1792	Note: in the context of a *record*, this quality implies that a record is what it purports to be; it does not address the trustworthiness of the record's content as a statement of fact.
4617	**authorised user**
4618	A *user* who has permission to carry out the action be described.
4619	Note: the details depend on the context. Different users will have different permissions. MoReq2 does not assume anything about which users or which roles have which permissions. The permissions that authorise a user to carry out an action are granted by the organisation, according to its policies and business requirements.
1794	**capture**
4649	(1) The act of recording or saving a particular instantiation of a digital object (source: InterPares 2 Project Terminology Database).
4650	(2) Saving information in a computer system.
1795	Note: in the context of MoReq2, capturing *records* is used to mean all of the processes involved in getting a record into an ERMS, namely registration, classification, addition of metadata, and freezing the contents. The term is used more generally to mean inputting to the ERMS and storing other information such as metadata values.
3248	**case file**
3249	A file relating to one or more transactions performed in a structured or partly-structured way.
3732	Source: adapted from PRO Functional Specification of "case file" (Appendix 1 reference [2]).

ID	Text
1779	**13.1 Glossary**
3736	Note: there is no universally-accepted definition of these terms, nor of the distinction between case files and the other kinds of files often managed by an ERMS. The following is therefore developed for, and intended to facilitate the understanding of, MoReq2; its applicability in other situations is not guaranteed.
3735	Note: the records in a case file may be structured or unstructured. The key distinguishing characteristic of case files is that they result from processes which are at least partly structured. Examples include files about: • applications for permits, etc.; • enquiries about a routine service; • investigation of an incident; • regulatory monitoring.
3734	Note: typically, other characteristics of case files are that they often: • feature a predictable structure for their content; • are numerous; • are structured or partly structured; • are used and managed within a known and predetermined process; • need to be retained for specific periods, as a result of legislation or regulation; • can be opened and closed by practitioners, end-users or data processing systems without the need for management approval.
3733	**case worker**
4345	A *user* who works with *case files*.
1796	**class**
1797	(in this specification only) The portion of a hierarchy represented by a line running from any point in the *classification scheme* hierarchy to all the files below it.
1798	Note: this can correspond, in classical terminology, to a "primary class", "group" or "series" (or sub-class, sub-group, sub-series etc.) at any level in the classification scheme.
1799	**classification**
1800	In records management, the systematic identification and arrangement of business activities and/or *records* into categories according to logically structured conventions, methods, and procedural rules represented in a classification system.
1801	Source: ISO 15489 (see Appendix 1 reference [9]).
4169	**classification code**
4563	An identifier given to each *class* in a *classification scheme*. Within each class, the classification codes of its descendant classes are unique.
1802	**classification scheme**
1803	See classification.
1804	Source: definition of "Classification System" in ISO 15489 (see Appendix 1 reference [9]).
1806	**clearance**
1807	See security clearance.
1808	**close** (verb)
1809	The process of changing the attributes of a *file, sub-file or volume* so that it is no longer able to accept the addition of *records*.
1810	**closed**
1811	Describes a *file, sub-file or volume* which has been closed and so cannot accept the addition of *records*.
2873	**component**
2874	A distinct byte stream that, along with other byte streams, makes up a *record* or *document*.
2876	Note: This term is not in general use.

ID	Text
1779	**13.1 Glossary**
2875	Note: The phrase "distinct byte stream" is used to describe what is usually called a "file" in information technology; the word "file" is avoided here to prevent confusion with the records management meaning of "file". The key concept is that a "component" is an integral part of the content of a record, despite the fact that it can be handled and managed separately. Note: Examples of components include: • An html document and JPEG images that make up a web page; • A word processing document and a spreadsheet, where the record consists of the word processing document that contains an embedded link (a hyperlink) to the spreadsheet.
3812	Note: components have to be distinct, i.e. separate from each other. If a word processed document contains an embedded spreadsheet (as opposed to an embedded link to a spreadsheet) then the spreadsheet is not considered to be a component; in this case, the word processed document complete with its embedded spreadsheet is a record made up of one component.
1812	**configuration time**
1813	The point in the lifecycle of the ERMS at which it is installed and its parameters are established.
4615	**custodian**
4616	(of a record or aggregation) the person or organisational unit having possession of the record(s).
1814	**destruction**
1815	Process of eliminating […] records, beyond any possible reconstruction.
1816	Source: ISO 15489 (see Appendix 1 reference [9]).
1817	**digital**
4601	Describes information expressed in binary notation.
1818	Note: this term is not used in MoReq2. Although "digital record" is more accurate than "electronic record", the former is rarely used in practice. See *electronic.*
3004	**disposition**
3005	Range of processes associated with implementing *records* retention, *destruction* or *transfer* decisions which are documented in retention and disposition schedules or other instruments.
3006	Source: ISO 15489 (see Appendix 1 reference [9]).
1819	**document** (noun)
1820	Recorded information or object which can be treated as a unit.
1821	Source: ISO 15489 (see Appendix 1 reference [9]).
1822	Note: a document may be on paper, microform, magnetic or any other electronic medium. It may include any combination of text, data, graphics, sound, moving pictures or any other forms of information. A single document may consist of one or several data objects.
1823	Note: documents differ from *records* in several important respects. MoReq2 uses the term document to mean information that is not a record.
4620	**document type**
4621	Describes *documents* that share common characteristics.
4622	Note: for example, documents with common layout, content, retention and disposition requirements, and/or *metadata*. Document types could include, for example: • application form; • correspondence (includes letters and faxes and memoranda); • curriculum vitae; • e-mail message; • invoice; • medical report; • web page.

ID	Text
1779	**13.1 Glossary**
4623	Note: in this example, e-mail messages are treated differently than other correspondence, as they may have different metadata requirements; this will not be the case in every organisation.
4624	Note: each organisation needs to define its document types, according to its business needs; the above are purely illustrative.
1824	**EDMS**
1825	Electronic Document Management System.
4602	Computer-based application dealing with the management of documents throughout the document life cycle
4603	Source: IEC 82045-1 Document Management.
1826	Note: the functionality required for EDMS is not included in this specification. However, an EDMS is often used in tight integration with an *ERMS*. See section 10.3 for more details.
1827	**electronic**
1828	For the purposes of this specification, the word "electronic" is used to mean the same as "digital".
1829	Note: analogue recordings, though they may be regarded as electronic, are not considered as "electronic" for the purposes of this specification as they cannot be stored within a computer system unless they are converted to digital form. It follows that, in the terminology of this specification, analogue records can only be stored as *physical records.*
1830	**electronic document**
1831	A *document* which is in electronic form.
1832	Note: use of the term *electronic document* is not limited to the text-based documents typically generated by word processors. It also includes e-mail messages, spreadsheets, graphics and images, HTML/XML documents, multimedia and compound documents, and other types of office document.
1837	**electronic record**
1838	A *record* which is in *electronic* form.
1839	Note: it can be in electronic form as a result of having been created by application software or as a result of digitisation, e.g. by scanning.
1840	**ERMS**
1841	Electronic Record Management System.
1842	Note: ERMS differ from *EDMS* in several important respects. See section 10.3 for more details.
1843	**export** (noun)
1844	The process of producing a copy of electronic *records*, along with their *metadata*, for another system.
1845	Note: the records remain on the ERMS after export, unlike *transfer*.
1846	**extract**
1847	(of a *record*) A copy of a *record* to which some changes have been applied to remove or mask but not to add to or meaningfully amend existing content.
1848	Source: definition of "instance" in PRO Functional Specification (Appendix 1 reference [2]).
1849	Note: the changes usually result from restrictions on disclosure of information. For example, a *record* may be made available only after individuals' names are masked or removed from it; in this case, an *extract* of the record is created in which the names have been made illegible. The process of masking is sometimes referred to as *redaction*.
1850	**file** (noun)
4174	An organised unit of *records* grouped together because they relate to the same subject, activity or transaction.
4604	Source: shortened and adapted from ISAD(G) (see Appendix 7.1).
4564	Note: this is the Records Management usage of the term *file*. It differs from the IT usage, for which MoReq2 uses the term *distinct byte stream.*

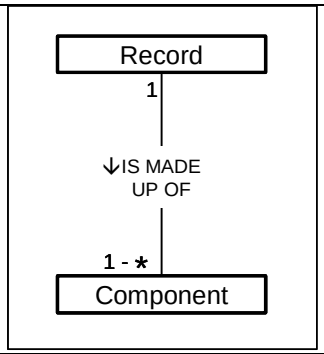
ID	Text
1779	**13.1 Glossary**
3743	**file format**
3744	The internal structure and/or encoding of a file which allows it to be interpreted or rendered into human-accessible form.
	Note: examples include: • HTML v3.2 (a file format for web pages); • PDF/A v1 (an archival file format for portable documents); • TXT (ASCII plain text file format); • XML v1.0 (a file format for extensible markup language which itself relies on ASCII plain text). • Many proprietary formats produced by desktop applications such as office suites.
3745	**format**
3746	See *file format*.
3250	**group** (noun)
3251	A set of *users*.
1856	**metadata**
1857	(in the context of records management) Data describing context, content and structure of records and their management through time.
1858	Source: ISO 15489 (see Appendix 1 reference [9]).
1859	Note: the distinction between data and its metadata can be unclear. For example, it is usually clear that the essential indexing data for a record (title, date etc.) is part of that record's metadata. However, the audit trail for a record, or the Retention and Disposition Schedule for a record, can validly be considered to be either data or metadata, depending on the context. Different types of metadata can be defined, for example, for indexing, for preservation, for rendering etc. These details of metadata usage are beyond the scope of MoReq2.
4570	**metadata stub**
4571	The subset of the metadata for an item that is retained after the item has been disposed of, to act as evidence that the item used to be held and has been properly disposed of.
3252	**non-case file**
3253	Any file that is not a *case file*.
1860	**open**
1861	(verb) The process of creating a new *file, sub-file or volume* such that it can accept the addition of records.
1862	(adjective) Describes a *file, sub-file or volume* which has not yet been *closed*, and so is able to accept the addition of *records*.
4611	**owner**
4612	The person or role responsible for a record or aggregation.
4613	Note: this is the usage in MoReq2; the legal owner of a *record* is the organisation that holds the record.
4614	Note: se also *custodian*.
1863	**paper file**
1864	A device for holding physical *documents* and *physical records*.
1865	Source: Adapted from PRO Functional Specification (Appendix 1 reference [2]).
1866	Note: examples of physical files include, among others, envelopes, box files and ring binders.
1867	**PDF**
1868	Portable Document Format, a *file format* for the representation of two-dimensional information.
1869	Note: this file format is proprietary to Adobe Inc., but is widely used. Its inclusion in this glossary does not represent any form of endorsement.
3010	**PDF/A**

ID	Text
1779	**13.1 Glossary**
3011	A subset of *PDF* designed for archival use, as defined in the ISO 19005 series of standards.
4545	**physical record**
4548	A *record* that is held in a medium outside the *ERMS*, such that the record itself is not under the management of the ERMS.
4546	Note: examples include paper records, microform records, and electronic records held on removable media so long as the records are not individually managed by the ERMS.
4547	**presentation**
1886	The manifestation of an *electronic record* presented by the ERMS to which a *user* can refer.
1887	Note: this may include on-screen display, printed and audio and multimedia presentations.
1888	Note: the exact nature of the presentation can be affected by the software and hardware environment. Typically different renditions of the same *record* can vary in details of font metrics, line endings and pagination, resolution, bit depth, colour space etc. In most cases these differences are acceptable. However, in some cases their potential effects have to be considered separately; these considerations are beyond the scope of this specification.
3752	Note: In the previous version of MoReq the term *rendition* was used with this meaning.
4207	**profile**
4208	The set of permissions allocated to a *user* or *group* or *role*.
1870	**record** (noun)
1871	Information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business.
1872	Source: ISO 15489 (see Appendix 1 reference [9]).
1873	Note: Local national definitions may also apply.
1874	Note: a record may incorporate one or several *documents* (e.g. when one document has attachments), and may be on any medium in any format. In addition to the content of the document(s), a record should include contextual information and, if applicable, structural information (i.e. information which describes the components of the record). A key feature of a record is that it cannot be changed.
4605	Note: both *electronic records* and *physical records* can be managed by an *ERMS*.
4186	**record type**
4187	Describes a *record* made from a *document* with the corresponding *document type*.
1875	**redaction**
1876	The process of hiding sensitive information in a *record*.
1877	Note: this can include applying opaque rectangles to obscure names etc. (the electronic equivalent of censoring paper documents with ink), more secure methods of obscuring information, or removing individual pages.
1878	Note: in all cases the totality of the original *electronic record* is not affected. Redaction is carried out on a copy of the electronic record; this copy is called an *extract*.
1879	**registration**
1880	The act of giving a *record* a unique identifier on its entry into a system.
1881	Source: ISO 15489 (see Appendix 1 reference [9]).
1882	Note: registration usually implies the recording into a "register" of important metadata, e.g. "all the data necessary to identify the persons and acts involved and the documentary context of the records" (UBC-MAS Glossary, Appendix 1 reference [x]).
1883	**render**
1884	The process of producing a *rendition*.
1885	**rendition**
3835	A manifestation of a *record* in a *file format* different from the record's native *file format*.

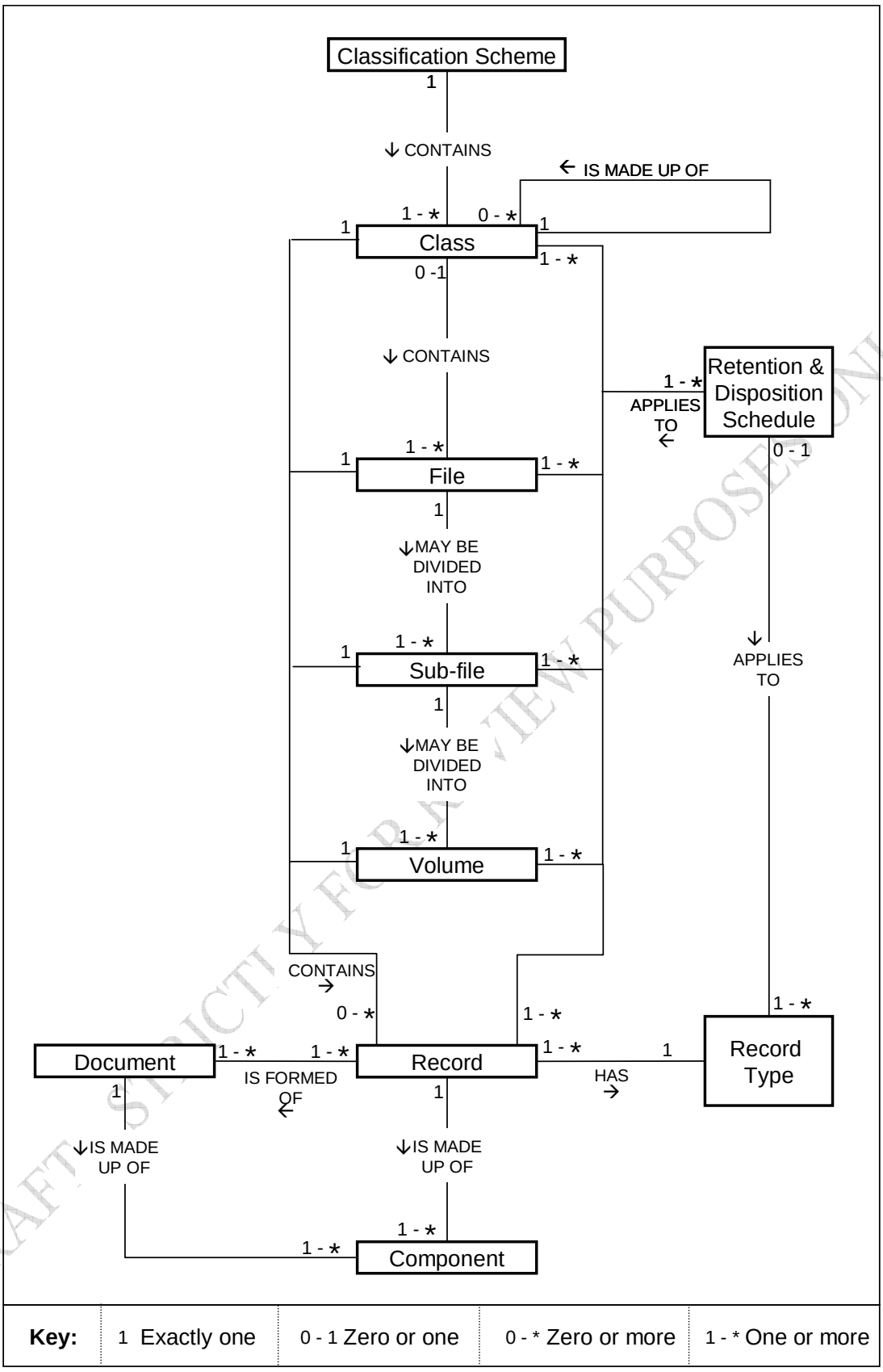
ID	Text
1779	**13.1 Glossary**
3836	Note: Renditions are usually produced to preserve electronic records, that is to minimise the risk of loss of access to their content over time. For example, records produced in a proprietary file format may be stored as renditions in a standard format such as PDF/A or xml.
3837	Note: Rendition was used with a different meaning in the original version of MoReq.
1889	**repertory**
1890	A list of existing *file* titles within each of the lowest levels of the classification scheme.
1891	**retention and disposition schedule**
3009	A formal instrument that defines the retention periods and consequent disposition actions authorised for *records* described in the schedule.
3008	Source: adapted from National Archives of Australia recordkeeping glossary.
1892	Note: in the previous version of MoReq this was referred to as a retention schedule.
1894	**role**
1895	The aggregation of functional permissions granted to a predefined subset of users.
1896	Source: PRO Functional Specification (Appendix 1 reference [2]).
1897	**security category**
1898	One or several terms associated with a *record* or *aggregation* which define rules governing access to it.
1899	Note: security categories are usually assigned at an organisational or national level. Examples of security categories used in government organisations throughout most of Europe are: “Top Secret”, “Secret”, “Confidential”, “Restricted”, “Unclassified”. These are sometimes supplemented by other terms such as “WEU Eyes Only” or “Personnel”.
1900	Note: this term is not in general use. It has been adopted in MoReq2 instead of the term “classification” that is often used by the security community to avoid confusion with the records management meaning of *classification*.
1901	**security clearance**
1902	One or several terms associated with a *user* which define the *security categories* to which the *user* is granted access.
4572	**stub**
4573	See *metadata stub*.
3012	**sub-file**
3013	Intellectual subdivision of a file.
3014	Note: Sub-files are usually used in case file management environments. Typically, each sub-file is named, and each sub-file is used to store a specified kind or kinds of records, such as “invoices”, “assessments” or “correspondence”.
1906	**transfer** (verb)
1907	The process of moving complete *electronic files*, along with their *metadata*, to another system.
1908	Source: adapted from PRO Functional Specification (Appendix 1 reference [2]).
1909	Note: the files are often transferred together with all other files in a *class* of the *classification scheme* when the purpose of transfer is to move the files to an archive for permanent preservation.
1910	Note: see also *export*.
1911	**user**
1912	Any person utilising the *ERMS*.
1913	Note: this may include (among others) Administrators, office staff, members of the general public and external personnel such as auditors.
3254	Note: a user may both have *roles* and be a member of *groups*.
4608	**user profile**
4609	The *profile* of a *user*.

ID	Text
1779	**13.1 Glossary**
3255	**user role**
3257	A set of functional permissions allocated to *users* allowed to perform actions that manage records.
4610	A *user* may have several *user roles* but has only one user profile.
3258	Note: In MoReq2 this term is used also to specify the people with these permissions.
1914	**version**
1915	(of a *document*) The state of a document at some point during its development.
1916	Source: PRO Functional Specification (Appendix 1 reference [2]).
1917	Note: a version is usually one of the drafts of a *document*, or the final document. In some cases, however, finished documents exist in several versions, e.g. technical manuals. In other cases, the versions are translations. By contrast *records* cannot exist in more than one version; see also *extract*.
1918	**volume**
1919	A subdivision of a *file*.
1920	Source: Definition of "part" in PRO Functional Specification (Appendix 1 reference [2]).
1921	Note: the subdivisions are created to improve manageability of the file contents by creating units which are not too large to manage successfully. The subdivisions are mechanical (e.g. based on number of records or ranges of numbers or time spans) rather than intellectual.

13.2 Entity-Relationship Model

ID	Text
1922	**13.2 Entity-Relationship Model**
1923	This section repeats part of section 2.3, for ease of reference.
1924	It contains an entity-relationship model which can be used as an aid to understanding the specification. Section 13.3 contains a narrative explanation that describes and explains the model.
1925	An important aspect of this diagram is that it need not represent actual structures stored in the ERMS. It represents a theoretical view of the entities associated with records. An ERMS uses these relationships to produce behaviour equivalent to the structures in the diagram. See section 2.2 for further explanation of this point.
1926	The relationships between files, volumes, records and other important entities are depicted in the following entity-relationship diagram. This is a formal representation of selected structures which can be used to describe the behaviour of an ERMS.
1927	In the diagram, entities - files, records and so on - are represented by rectangles. The lines connecting them represent the relationships between the entities. Each relationship is described by text in the middle of the line; and this should be read in the direction of the arrow. Each end of the relationship has a number which represents the number of occurrences (strictly, the cardinality); the numbers are explained in the key. So, for example, the following extract:
2944	

ID	Text
1922	**13.2 Entity-Relationship Model**
1928	means “one record is made up of one or more components” (note the direction of the relationship arrow).
1929	Note also that the entity Class is related to itself by the relationship “is made up of”. This relationship describes, in formal terms, the relationship between classes in a hierarchical classification scheme, where a Class may be made up of one or more other Classes. If this relationship (sometimes called a recursive relationship) is removed, the model applies equally to non-hierarchical relationships.
2931	**Note to reviewers: the entity-relationship diagram that follows is significantly different to the corresponding diagram in MoReq.**
2945	



v4

13.3 Entity Relationship Narrative

ID	Text
1930	**13. 3 Entity Relationship Narrative**

ID	Text
1930	**13. 3 Entity Relationship Narrative**
1933	The preceding diagram shows a simplified model; it does not attempt to represent all possible entities or relationships. Rather, it shows only the most significant ones for this application. For example, it does not show users, roles etc.
1934	The remainder of this narrative describes the entities in the diagram, and their inter-relationships.
1935	**Classification Scheme**
1936	In order to practice records management principles, an organisation must have at least one classification scheme. This sets out the filing structure (typically consisting of hierarchy) for a defined part of the organisation.
1939	**Class**
1940	Hierarchical classification schemes can be viewed as a hierarchy made up of a number of classes, much as a tree is made up of branches. Each class is connected to the hierarchy at one level; can extend over several levels; and can contain smaller classes. Several classes can start at any single level; but each class starts only at one level.
1941	**File**
1942	Files occur within classes, at any point in the hierarchy. At any point, there can be no files, one file or several.
1943	**Sub-file**
2927	Each file is viewed as being made up of at least one sub-file. In practice, some files are not divided into sub-files. Where there is only one sub-file, the concept of sub-file is transparent to users, for all practical purposes. Sub-files are used mainly in case files.
2928	**Volume**
1944	Sub-files can be divided into volumes, according to specific rules. In practice, most sub-files are not divided into volumes. Where there is only one volume, the concept of volume is transparent to users, for all practical purposes. The rules may depend on size or number of records, or may depend on transactions or time periods. This practice originated with physical files, in order to restrict them to a manageable size and weight. The practice is, where appropriate, continued with electronic files, to limit them to a manageable length for review, transfer, etc.
1945	The terms file, sub-file and volume are, in practice, sometimes used loosely or interchangeably - because of the above requirement for transparency. For example, a user will typically ask for “a file” rather than (more accurately) asking for “a volume.” This is especially apparent in the case of a physical file that consists only of a single one-volume sub-file. In this case, although the file analytically consists of one sub-file which is made up of one volume, the sub-file and the volume are not always labelled as such (often, the label is only applied when the second sub-file or volume is opened). Strictly, all end users interact with volumes, but this is often simplified to files.
1946	**Retention and Disposition Schedule**
1948	A retention and disposition schedule specifies the rules for keeping and disposing of records. The ERMS can contain several retention and disposition schedules, one or more of which are applied to each class, file, sub-file and volume; they can also be applied to records, and one retention and disposition schedule may be applied to each record type.
1949	**Record**
1950	At the heart of the system lies the most important entity, the records. These are the reason for the entire records management infrastructure, as they form the account of the organisation's activities.
1951	Records are made from documents. Each record can comprise one or several documents; and each document can appear in several records.
2929	**Record Type**

ID	Text
1930	**13. 3 Entity Relationship Narrative**
2930	Records are assigned a record type. This is used to indicate, and to allow the ERMS to manage, the records in certain ways. Examples of record type might include “invoice” and “web page”.
2932	**Component**
2933	Each record and document is made up of at least one component; some are made up of more than one. For example, a simple web page may consist of only one component - an HTML "file" in IT terms - while a more complex web page may consist of dozens - an HTML “file”, GIF “files”, JPEG “files” and so on.

13.4 Access Control Model

ID	Text
1959	**13.3 Access Control Model**
1960	This section contains a simple model of example roles within an ERMS.
3278	The matrix recognises two main roles, which are themselves divided into roles. The main roles are user roles and administrative roles. These are defined in terms of access to ERMS functionality.
	The number of roles shown in this model is only illustrative. It is not meant to indicate that any organisation should implement these roles, not that any organisation should implement this number of roles. Each organisation should define the roles it needs; and these needs will tend to vary over time.
3279	The below roles illustrate an example of access control rights for specific aspects of system functionality according to organisational responsibilities.
3242	There are four example roles defined in the example matrix: • Central Administrator - this role has control over the configuration of the entire ERMS and the management of the aggregations and records themselves. • Local Administrator - this is a role with administrative rights over a sub-set of the ERMS or its classification scheme. These roles usually are useful in geographically dispersed organisations. • Reviewer - this is a specialist role which is primarily concerned with the application of disposition actions defined by Retention and Disposition Schedules. • End User - the end user role is the standard level of access to the ERMS and comprises those who need to save records into, and access records from, the ERMS for their routine work.
1961	Administrative roles are here divided into two roles only as an example; responsibilities can be divided in other ways. For some small organisations this division might be needlessly complicated, as only one person, with a single role, can manage all the administration. For large organisations it might be an over-simplification because more than two roles are needed (such as Records Manager, Records Officer, Archivist and Data Manager or IT Manager). MoReq2 does not attempt to specify how many administrative roles would be needed in any real organisation.
3243	The role of Local Administrator is given here as an example of one of these. This role can also have several titles in different organisations. In some cases this may be a Local Records Officer, or a Super-user etc.
1962	In any event, administrative roles are only implementing, from a system perspective, decisions taken by more senior management. Such decisions are typically based on the organisation's business requirements and records policy. The decisions also are informed by laws and regulations, such as information laws, data security laws, archival laws and industry regulations; these are addressed in section <11.5>.
3280	This matrix is not intended to imply that administrative roles must take management decisions, though in some environments that may be the case.

ID	Text
1959	**13.3 Access Control Model**
1963	Administrative roles take actions related to the management of records themselves; their interest is in managing records as entities rather than their content or business context. They may also manage the ERMS hardware, software and storage, ensure backups are taken and manage the performance of the ERMS.
4185	Many organisations also need to integrate the management of business processes with the management of records. In this case there is scope to allocate a particular set of administrative permissions to individual business managers. This could include the ability to monitor and manage a specific group of users or area of the classification scheme.
3285	Although MoReq2 refers to a user role there will be, in the majority of organisations, a number of different user roles and the ERMS should not limit the number of roles that can be configured.
4184	One example of this could be that of a case worker See chapter 10.6 Casework). Such a role would have specific permissions within a particular branch of the classification scheme.
3281	Unlike administrative roles, user roles have access to facilities which an office worker or researcher needs when using records. This includes adding documents, searching for and retrieving records. Their interest is primarily in the contents, properties or business context of records rather than their management – in other words, they are interested in the business processes evidenced by the records.
3282	In the matrix, the role of end user shows the access rights that typically are appropriate for the majority of users in an organisation to carry out their business functions.
3283	A further example of a user role is given: reviewer. This shows a level of access control that may be allocated to a sub-set of users for the purposes of reviewing records.
1969	This matrix is best viewed as a starting point, and as the formal basis for assigning rights. Users of this specification will need to consider additional requirements which are specific to their environment.
3286	The formal requirements dealing with this table are at the end of chapter 4; they confirm that **the requirement is not for an ERMS to incorporate the sample access matrix shown here, but to be capable of being configured to at least this level of detail,** for an unrestricted number and type of roles and functions. It must be possible to configure each cell of the matrix as "yes" or "no", but with the table having as many columns as the organisation needs..
	Other possible roles that might be implemented by organisations include but are not limited to: • assistant; • auditor; • freedom of information manager; • manager; • records creator; • records manager • supervisor.
1968	This matrix is divided into sections. These sections group, for convenience, the functions normally associated with files, records, records management and administration.
3241	-

Example Access Matrix illustrating Level of Detail		
	Users	
	User Roles	Administrative Roles

Function	End User	Reviewer	Local Administrator	Central Administrator
Add new classes	No	No	Yes	Yes
Create new files	Yes	No	Yes	Yes
Change file metadata	No	Yes	Yes	Yes
Maintain classification scheme and files	No	No	Yes	Yes
Delete files	No	No	Yes	Yes
Capture records	Yes	No	Yes	Yes
Relocate a record to a different file	Yes	No	Yes	Yes
Search for and read records	Yes	Yes	Yes	Yes
Change content of records	No	No	No	No
Change record metadata	No	Yes	Yes	Yes
Delete records	No	No	Yes	Yes
Place and remove disposal holds	No	Yes	Yes	Yes
Retention and disposition schedule and disposal transactions	No	Yes	Yes	Yes
Export and import files and records	No	Yes	Yes	Yes
View audit trails	No	Yes	Yes	Yes
Configure and manage audit trail	No	No	No	Yes
Change audit trail data	No	No	No	No
Move audit trail data to off-line storage media	No	No	Yes	Yes
Perform all transactions related to users and their access privileges	No	No	Yes	Yes
Allocate access controls to local administrators	No	No	No	Yes
Allocate own access controls also to other users	Yes	Yes	Yes	Yes
Maintain database and storage	No	No	Yes	Yes
Maintain other system parameters	No	No	No	Yes
Define and view other system reports	No	Yes	Yes	Yes

Figure <C13.4 ID3241>

Appendix 7 – Standards and Other Guidelines

7.1 – Standards

ID	Text
3143	**Appendix 7.1 - Standards**
3613	This annex lists standards and other resources referenced in the specification or applicable to electronic records management.
4527	The standards include those that are particularly relevant to ERMSs; they omit generic standards such as those dealing with storage hardware and database languages.
4528	The standards include international standards, both de jure and de facto. National standards are omitted from this list. They may be added to a chapter zero by the authority for a member state. Only standards that have a direct bearing on systems design are included; standards that address organisation and ongoing management are not included.
3143	**Appendix 7.1 – Standards**
3681	

EAD	Encoded Archival Description.
ISAAR(CPF)	International Standard Archival Authority Record for Corporate Bodies, Persons, and Families (International Council on Archives).
ISAD(G)	General International Standard Archival Description, Second Edition (International Council on Archives).
IETF RFC 2821	Simple Mail Transfer Protocol. (http://www.ietf.org/rfc/rfc2821.txt)
IETF RFC 2822	Internet Message Format. (http://www.ietf.org/rfc/rfc2822.txt)
ISO 216	Writing paper and certain classes of printed matter -- Trimmed sizes -- A and B series
ISO 639	Codes for the representation of names of languages.
ISO 3166	Codes for the representation of names of countries.
ISO 2788	Guidelines for the establishment and development of monolingual thesauri.
ISO 5964	Guidelines for the establishment and development of multilingual thesauri.
ISO 8601	Representation of dates and times.
ISO 9834-8	Generation and registration of Universally Unique Identifiers (UUIDs) and their use as ASN.1 Object Identifier components. (see also ITU X.667)
ISO 10196	Document imaging applications -- Recommendations for the creation of original documents
ISO 12033	Guidance for selection of document image compression methods.
ISO 12037	Recommendations for the expungement of information recorded on write-once optical media.
ISO 12142	Media error monitoring and reporting techniques for verification of stored data on optical digital data disks.
ISO 12654	Recommendations for the management of electronic recording systems for the recording of documents that may be required as evidence, on WORM optical disk.
ISO 14721	Space data and information transfer systems – Open archival information system - Reference model (OAIS).

ISO 15444	JPEG 2000 image coding system: Core coding system.
ISO 15489	Records Management.
ISO 15801	Information stored electronically -- Recommendations for trustworthiness and reliability.
ISO 15836	The Dublin Core metadata element set.
ISO/IEC 18019	Guidelines for the design and preparation of user documentation for application software (see especially clause 4.2.6). (Due to be replaced by ISO/IEC 26514.)
ISO 18492	Long-term preservation of electronic document-based information.
ISO 19005-1	Electronic document file format for long-term preservation - Part 1: Use of PDF 1.4 (PDF/A-1).
ISO/DIS 22938	Electronic content/document management data interchange format.
ISO 23081	Metadata for records.
ISO 23950	Information retrieval - application service definition and protocol specification.
ISO 26300	Open Document Format for Office Applications (OpenDocument) v1.0.
ISO/IEC 26514	User documentation requirements for documentation designers and developers. (Under development.)
ITU X.667	Generation and registration of Universally Unique Identifiers (UUIDs) and their use as ASN.1 object identifier components. (http://www.itu.int/ITU-T/studygroups/com17/oid/X.667-E.pdf).
TIFF	Tagged Image File Format. (http://partners.adobe.com/public/developer/tiff/index.html)
X.509	ITU-T Recommendation X.509: Open systems interconnection – The Directory: Public-key and attribute certificate frameworks. (http://www.itu.int/rec/T-REC-X.509-200003-I/en).
XKMS	XML Key Management Spec. (http://www.w3.org/TR/xkms/).
XML	W3C Extensible Markup Language (XML)(http://www.w3.org/TR/REC-xml/).

7.2 - Other Guidelines

ID	Text
3720	**Appendix 7.2 - Other Guidelines**
3721	

ISO 9241-171	Ergonomics of human-system interaction - Part 171: Guidance on software accessibility
ISO/TS 16071	Guidance on accessibility for human-computer interfaces (due to be superseded in 2007 by ISO 9241).
WfMC	Workflow Management Coalition Terminology & Glossary. (http://www.wfmc.org/standards/referencemodel.htm).

7.3 - Accessibility Guidelines and Resources

ID	Text
3722	**Appendix 7.3 - Accessibility Guidelines and Resources**
	This section lists guidelines and resources for developers and purchasers of

	ERMSs. Whereas other sections of this Appendix contain only open and international publications, this section includes information that is originally national and that originates from the supplier community. This is because no internationally-accepted documentation has been identified; these may be added in any later editions of MoReq.
3723	

For developers
W3C Web Content Accessibility Guidelines (for websites and web applications) http://www.w3.org/WAI/
RNIB Web Access Centre http://www.rnib.org.uk/webaccesscentre
RNIB Software Access Centre http://www.rnib.org.uk/softwareaccesscentre
IBM Human Ability and Accessibility Centre http://www-03.ibm.com/able/guidelines/
For procurement
ACCENT - Accessibility in ICT Procurement: EU project http://www.verva.se/web/t/Page____2936.aspx (note: there are four "_" underscore characters in the above url)
PAS 78:2006 Publicly Available Specification for commissioning accessible websites http://www.drc-gb.org/library/website_accessibility_guidance.aspx
RNIB Software Access Centre http://www.rnib.org.uk/softwareaccesscentre

Appendix 9: Metadata Model

ID	Text
4396	**Appendix 9: Metadata Model**
4445	This appendix describes the MoReq2 metadata model. It is significantly different from the model in MoReq. Accordingly there is no cross-reference between the two models.
4444	The purpose of the MoReq2 metadata model is to define the metadata needed to allow exchange of records between ERMSs with no loss of MoReq2-related mandatory functionality (with one exclusion, explained below).
4443	This metadata model excludes the metadata necessary to define the user access rights model. This is because; • MoReq2 does not mandate an access control model; instead it specifies a general framework within which a specific model should be constructed (section 12.4); • User identities are not generally transportable across systems, and so cannot be meaningfully included here.
4442	The metadata model is described in terms of a minimum set of metadata "elements" These "elements" are those that the ERMS must be able to export, import, and process. An "element", referred to as "field" in the past, is the variable used to hold a metadata "value". So examples of elements and metadata values are:
4441	

Example of metadata element	Examples of possible metadata values
Title	Request for permission to release ABC *or* Report on failure of DEF system *or* Complaint about GFI
Identifier	N1128A *or* 3F2504E0-4F89-11D3-9A0C-0305E82C3301 *or* 7QDBkvCA1+B9K/U0vrQx1A
Keyword	Records, Archives, Information *or* Air travel *or* Recreational activity, sport, field events, javelin

4440	Almost any ERMS can be configured with sufficient fields to support the metadata elements listed below; however, this alone is insufficient. It is important that: • the ERMS must use the metadata elements to enable and support the functionality defined in the remainder of this specification (see <MoReq2 requirement 12.1.2>); • the ERMS must include features supporting validation, inheritance and default value rules when capturing the metadata elements.
4439	This model stops short of being a complete schema or application profile for ERMS metadata. An xml schema is the subject of a separate, related, development <insert footnote reference or similar to xml schema>.

Audit Trail

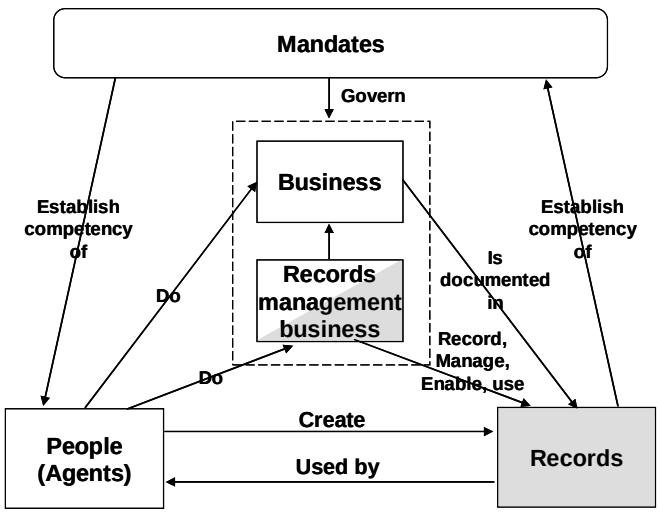
ID	Text
4438	**Audit Trail**
4437	For the purposes of this model, audit trail information is not considered to be metadata.

Implicit and Explicit Metadata

ID	Text
4436	**Implicit and Explicit Metadata**
4435	The MoReq2 Metadata Model specifies minimum metadata needed for compliance with MoReq2. This is intended to represent the minimum metadata required for good records management. However, MoReq2 compliance doe not mean that values for all the elements specified in this model must be stored explicitly in a metadata database. It does mean that the ERMS must be capable of exporting, importing, and processing the values. Therefore, it is acceptable for metadata values to be stored implicitly by the ERMS. This is illustrated in two examples.
4434	• The identifier of the retention and disposition schedule that applies to a file can be stored explicitly as a metadata value in a metadata database, as a value associated with the file. However, it is acceptable for the identifier to be stored in the database as a value associated with the file's parent class, in other words as a value implicitly associated with the file through inheritance.

4433	• The title of a record can be stored explicitly as a metadata value in a metadata database, as a value associated with the record. However, it is acceptable for ERMS not to store the title explicitly if the title is stored as a part of the record itself (so long as the ERMS is able to process the title).

Principles

ID	Text
4432	**Principles**
4431	The MoReq2 metadata model is intended to be consistent, to the extent possible, with the following international standards:
4430	• ISO 23081 – Records management processes – Metadata for records;
4429	• ISO 15489 – Records management;
4428	• ISO 15836 – The Dublin Core metadata element set.
4427	For several reasons, the MoReq2 metadata model does not comply fully with these three standards. Reasons include:
4426	• The scope of ISO 23081 is greater than the scope of MoReq2; it therefore describes more metadata than is defined in the MoReq2 metadata model.
4425	• The metadata elements specified in ISO 15836 are not sufficient for records management, and are not all well-suited to records management use;
4424	• ISO 23081-2 was published after the MoReq2 project started;
4423	• MoReq2 extends the management of records to areas not covered by these standards, notably in its inclusion of sub-files and volumes.
4422	ISO 23081 defines six "types" of metadata, as follows:
4421	"a) Metadata about the record itself; b) Metadata about the business rules or policies and mandates; c) Metadata about agents; d) Metadata about business activities or processes; e) Metadata about records management processes; and f) Metadata about the metadata record."
4420	The MoReq2 metadata model covers most of a), part of e), and part of f).
4419	ISO 23081 partially represents the six "types" of metadata in a diagram; this is reproduced below, with the addition of shading that represents the parts of the model covered by MoReq2.
4418	 Figure <A9 ID4418>

4417	**Insert footnote**: ISO 23081 attributes this diagram as follows: Derived from Figure 2 Recordkeeping and Figure 3 The Business Context, included in "Conceptual and Relationship models: Records in Business and Socio-legal Contexts", a deliverable from the 1998-1999 Monash University research project, called "Recordkeeping Metadata Standards for Managing and Accessing Information Resources in Networked Environments Over Time for Government, Commerce, Social and Cultural Purposes". Chief Investigators: Sue McKemmish, Ann Pedersen and Steve Stuckey. http://www.sims.monash.edu.au/research/rcrg/research/spirt/reports.html.
4416	In omitting some of the metadata types identified in ISO 23081, an MoReq2-compliant ERMS is at risk of compromising some aspects of the integrity of records. For example, ISO 23081-1 requires (in clause 9.3.1) that metadata recorded at the time a record is captured should:
4415	"a) identify the specific metadata scheme or schema used in organisational business systems, b) capture the business rules or other system controls that regulate record creation and management, c) capture the business rules or other system controls that regulate metadata creation and management, d) capture the business rules or other system controls that regulate records management operations, e) capture the business rules or other system controls that regulate access, and rights to records, f) document the mandate or other regulatory requirement for record creation and/or management, g) document the mandate or other regulatory requirement for record retention, security or destruction requirements, and h) capture the links between the mandate or regulatory information and the records or records management processes to which it relates."
4414	However, the effort required to implement all the above completely is large. Users of MoReq2 are advised to evaluate the level of risk for their organisation. Where such risks are deemed unacceptable, ISO 23081 should be consulted for guidance on how to extend the metadata model. However, in most ERMS implementations the risks involved are likely to be acceptably low.

Presentational Conventions

ID	Text
4413	**Presentational Conventions**
4412	Strictly for the presentational reasons, the metadata elements are divided into several sections, as follows:
4411	• Section A9.2 covers metadata for classification schemes;
4410	• Section A9.3 covers metadata for classes, files, sub-files, volumes and records;
4409	• Section A9.4 covers metadata for retention and disposition schedules.
4408	• Section A9.5 covers metadata that is unique to record extracts;
	• Section A9.6 covers metadata stubs.
4407	Considerations for preservation metadata are in section A9.6. Notes on customisation of this model follow in A9.7.
4406	The metadata elements for classes, files, sub-files, volumes and records are brought together in one section, despite the fact that they are describing different sorts of entities. This is only for brevity and ease of presentation. In this section the noun "entity" is used to mean "any of class, file, sub-file, volume and record, as appropriate".
4405	Every metadata element is shown as one table, as in the following figure:

4404

Name

Number	**Obligation:**		**Occurs:**		
Definition:					
Applies to:	class	file	sub-file	volume	record
Populated:					
Use conditions:					
Comment:					
Requirements					

A9 <ID4404>

4403 Each table provides the following information about one metadata element:

- **Name:** the name given to the metadata element in MoReq2.
- **Number:** A unique three-digit number, preceded by the letter M (for example, M012). This can be used to refer to the element. The number is arbitrary.
- **Obligation:** whether a value for the element is mandatory or optional for compliance with MoReq2.
- **Occurs:** whether more than one value is allowed for the element (for example, a "title" element must have only one value, whereas "author" may have many. This is technically referred to as "cardinality."
- **Definition:** a short description of the element.
- **Applies to:** (section 12.4 only): to which of the entities class, file, sub-file, volume and record the element applies. A tick (✓) indicates that the element applies to the entity shown by the tick.
- **Populated:** the source of the value(s) for this element. and the event associated with the initial population of the element.
- **Use conditions:** conditions and rules that govern the value(s) of the element.
- **Comment:** additional information (for some elements only).
- **Requirements:** references to formal requirements from other chapters of MoReq2 that require the metadata element. In some cases the list of requirements may not be complete.

Naming Conventions

ID	Text
4402	**Naming conventions**
4401	Most of the elements have names formed in a way which is consistent with ISO 15836 (Dublin Core) principles.
4400	The first part of the name is a Dublin Core element name (e.g. Identifier, Subject). So, for example, the following Dublin Core names are used as MoReq2 metadata element names: • **Title:** a textual name or identifier, which can be unique or non-unique; • **Subject:** a topic.
4399	Note that in this model (as in others) an element name is unique within one section, but is not always unique across the entire model. This, for example, elements named "identifier" are found in the section on classification schemes and in the section on classes, files, sub-files, volumes and records.
4398	The second part refines the name, differentiating it from related elements. Complete consistency with Dublin Core is not possible, and could be seen as undesirable since Dublin Core metadata is largely concerned with discovery rather than with ongoing information management.

4397	Where an element name has two parts, they are separated by a full stop (the delimiter “.”). If a part of the name contains more than one English word they are separated by an underscore (the delimiter “_”).

Metadata Elements

<Metadata elements to be inserted here>