INTERNATIONAL STANDARD

ISO 16175-2

First edition
2011-04-15

Information and documentation — Principles and functional requirements for records in electronic office environments —

Part 2: Guidelines and functional requirements for digital records management systems

Information et documentation — Principes et exigences fonctionnelles pour les enregistrements dans les environnements électroniques de bureau —

Partie 2: Lignes directrices et exigences fonctionnelles pour les systèmes de management des enregistrements numériques

Reference number
ISO 16175-2:2011(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO 16175-2 was prepared by the International Council on Archives (as International Council on Archives and the Australasian Digital Recordkeeping Initiative *Principles and functional requirements for records in electronic office environments — Module 2: Guidelines and functional requirements for digital records management systems*) and was adopted, under a special “fast-track procedure”, by Technical Committee ISO/TC 46, *Information and documentation*, Subcommittee SC 11, *Archives/records management*, in parallel with its approval by the ISO member bodies.

ISO 16175 consists of the following parts, under the general title *Information and documentation — Principles and functional requirements for records in electronic office environments*:

— *Part 1: Overview and statement of principles*

— *Part 2: Guidelines and functional requirements for digital records management systems*

— *Part 3: Guidelines and functional requirements for records in business systems*

(Blank page)

International Council on Archives

Information and documentation - Principles and functional requirements for records in electronic office environments

Part 2

Guidelines and functional requirements for digital records management systems

Published by the International Council on Archives. This part was developed by Archives New Zealand in conjunction with a joint project team formed by members of the International Council on Archives and the Australasian Digital Recordkeeping Initiative.

ISBN: 978-2-918004-01-1

This publication should be cited as: International Council on Archives, *Principles and Functional Requirements for Records in Electronic Office Environments – Module 2: Guidelines and Functional Requirements for Electronic Records Management Systems,* 2008, published at www.ica.org

CONTENTS

INTRODUCTION

Effective management of records and information is fundamental to a well-functioning organisation as it supports business activity and provides a basis for efficient service delivery. It also provides the mechanism whereby organisations can account for their decisions and actions and retain corporate memory. Moreover, good records management is simply good business practice.

Digital records management systems facilitate:

a) efficiency, by making information readily available when needed for decision-making and operational activities;

b) sound use of financial resources, by allowing timely disposition of non-current records;

c) accountability, by enabling the creation of a complete and authoritative record of activities;

d) compliance, by demonstrating that legal requirements have been met; and

e) risk mitigation, by managing the risks associated with illegal loss or destruction of records, and from inappropriate or unauthorised access to records.

A fundamental underlying principle for this document, *Principles and functional requirements for records in electronic office environments – Part 2: Guidelines and functional requirements for digital records management systems*. (hereafter the term 'part' is used) is the distinction between business systems (or business information systems) and digital (or electronic) records management systems. Business systems contain data that is commonly subject to constant updates (dynamic), able to be transformed (manipulable) and contain data in current business use (non-redundant). By contrast, digital records management systems contain data that is not dynamically linked to business activity (fixed), unable to be altered (inviolable), and may be non-current (redundant). Therefore business systems are beyond the scope of this part (see *ISO1617-3: 2010, Information and documentation - Principles and functional requirements for records in electronic office environments – Part 3: Guidelines and functional requirements for records in business systems.).*

The records within a digital records management system are, however, still dynamic in the sense that they can be (re)used in new business activity/contexts, so new metadata will be added through the ongoing use of the record content. Digital records management systems provide the technological component of a framework for the systematic and structured management of records; they link digital and non-digital records to business activities, retain records of past actions, and fix the content and structure of records over time.

The primary audience for this document is staff responsible for designing, reviewing and/or implementing digital records management systems in organisations – whether

those systems are commercial off-the-shelf digital records management software applications, or custom-built applications.

This part primarily addresses the requirements of organisational records/information managers or system procurement project leaders, but will be relevant for jurisdictional standard-setters and the wider records management community.

Another key audience is software vendors and developers who market and/or develop digital records management system products. This part is intended to inform their decision-making when designing records management functionality within digital records management products.

1. SCOPE

The scope of this part is limited to products that are often termed ‘electronic records management systems’ or ‘enterprise content management systems’. This part will use the term digital records management systems for those software applications whose primary function is records management. It does not seek to set requirements for records still in use and held within business systems. Digital objects created by email, word processing, spreadsheet and imaging applications (such as text documents, and still or moving images), where they are identified to be of business value, should be managed within digital records management systems which meet the functional requirements set out in this part.

Records managed by a digital records management system may be stored on a variety of different media formats, and may be managed in hybrid record aggregations that include both digital and non-digital elements.

This part does not attempt to include requirements that are not specific to, or necessary for, records management, for example, general system management and design requirements. Nor does it include requirements common to all software applications, such as performance, scalability and usability. Given the target audience of this document, it also assumes a level of knowledge about developing design specifications, procurement and evaluation processes, and therefore these issues are not covered in this part. Although not included in this part’s requirements, the importance of non-records management functional requirements for records management systems is recognised through their inclusion in the high-level model outlined in Section 4.2: Overview of functional requirements.

Specifications for the long-term preservation of digital records are also beyond the scope of this part; this issue should be addressed separately within a dedicated framework for digital preservation or ‘digital archiving’ at a strategic level. These digital preservation considerations transcend the life of systems and are system independent; they should be assessed in a specific migration and conversion plan at the tactical level. However, recognition of the need to maintain records for as long as they are required shall be addressed, and potential format obsolescence issues should also be considered when applying the functional requirements.

This part articulates a set of functional requirements for digital records management systems. These requirements apply to records irrespective of the media in which they were created and/or stored. The requirements are intended to:

a) set out the processes and requirements for identifying and managing records in digital records management systems;

b) set out the records management functionality to be included in a design specification when building, upgrading or purchasing digital records management systems software;

c) inform records management functional requirements in the selection of commercially available digital records management systems; and

d) review the records management functionality of, or assess the compliance of, an existing digital records management system.

2. RELATED STANDARDS

The following documents are referenced for the application of this document.

ISO 15489-1:2001, *Information and documentation — Records management — Part 1: General*

ISO/TR 15801:2009, *Document management — Information stored electronically — Part 2: Recommendations for trustworthiness and reliability*

ISO16175-1:2010, *Information and documentation — Principles and functional requirements for records in electronic office environments — Part 1: Overview and statement of principles.*

ISO1617-3:2010, *Information and documentation - Principles and functional requirements for records in electronic office environments – Part 3: Guidelines and functional requirements for records in business systems.*

ISO 23081-1:2006, *Information and documentation — Records management processes — Metadata for records — Part 1: Principles*

ISO 23081-2:2009, *Information and documentation — Managing metadata for records — Part 2: Conceptual and implementation issues.*

ISO 2788:1986, *Documentation —* Guidelines *for the establishment and development of monolingual thesauri.*

ISO 5964:1985, *Documentation — Guidelines for the establishment and development of multilingual thesauri.*

International Council on Archives, *Principles and Functional Requirements for Records in Electronic Office Environments, Part 1 — Overview and Statement of Principles*, 2008.

International Council on Archives, *Principles and Functional requirements for Records in Electronic Office Environments, Part 3 — Guidelines and Functional Requirements for Records in Business information systems*, 2008.

3. TERMS AND DEFINITIONS

For the purposes of this document, the terms and definitions in ISO 15489-1:2001, ISO/TR 15801:2009, ISO 23081-1:2006 and ISO 23081-2:2009, and the following apply.

Term	Definition
Activity (business activity)	The second level of a business classification scheme. NOTE 1 Activities are the major tasks performed by an organisation to accomplish each of its functions. An activity is identified by the name it is given and its scope note. The scope of the activity encompasses all the transactions that take place in relation to it. Depending on the nature of the transactions involved, an activity may be performed in relation to one function, or it may be performed in relation to many functions.
Aggregation	Any accumulation of record entities at a level above record object.
Business classification scheme (BCS)	**Business classification scheme** The conceptual, hierarchical, representation of the functions and activities performed by an organisation. NOTE 1 A Business classification scheme is usually a taxonomy derived from the analysis of business activity.
Business activity	An umbrella term covering all the functions, processes, activities and transactions of an organisation and its employees. Includes public administration as well as commercial business.

Term	Definition
Business information system	An automated system that creates or manages data about an organisation's activities. NOTE 1 Business information systems are (often multiple or related) applications whose primary purpose is to facilitate transactions between an organisational unit and its customers, for example, an e-commerce system. client-relationship management system, purpose-built or customised database, finance or human resources systems. NOTE 2 Business information systems typically contain dynamic data, that is commonly subject to constant updates, able to be manipulated and holds 'current' data. NOTE 3 Although digital records management systems are business information they differ from most others in that their primary function is the management of records rather than to facilitate a business process.
Classification	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. NOTE 1 Classification includes determining document or file naming conventions, user permissions and security restrictions on records.
Component	A set of constituent parts that comprises a digital record.
Compound record	A record that comprises multiple digital objects.
Destruction	The process of eliminating or deleting records, beyond any possible reconstruction. NOTE 1 Destruction of digital records is a disposition process whereby digital records and their metadata are permanently removed, erased or obliterated as authorised and approved by a disposition authority schedule.
Digital file	A set of related digital records held in a tightly bound relationship within the business system and managed as a single object. NOTE 1 A type of aggregation of digital records, also referred to as a 'container'.

Term	Definition
Digital object	An object that can be represented by a computer, such as a file type generated by a particular system or software application. NOTE 1 A digital record may comprise one or more digital objects.
Digital records management system	An automated system whose primary function is to manage the creation, use, maintenance and disposition of digitally created records for the purposes of providing evidence of business activities. NOTE 1 These systems maintain appropriate contextual information (metadata) and links between records.
Disposition	A range of processes associated with implementing retention, destruction or transfer decisions which are documented in disposition or other instruments.
Function	The highest level of a business classification scheme. NOTE 1 Functions represent the major responsibilities that are managed by the organisation to fulfil its goals.
Hybrid file	A set of related digital files and physical files managed as a single entity.
Hybrid record	A record consisting of digital and non-digital components. NOTE 1 The digital record and its associated records management metadata is maintained within the digital records management system together with the records management metadata relating to the non-digital record.

Term	Definition
Marker	**Marker** A metadata profile of a record physically held outside of a digital system. NOTE 1 A marker may denote a physical record (such as a large bound volume or building plan) or a digital record stored on removable media (such as a CD-ROM or video). NOTE 2 A marker may act as a representational link to a relevant record within the digital records management system to alert users to the existence of a relevant record that is required to be accessible in more than one location.
Metadata	Structured or semi-structured information, which enables the creation, management and use of records through time and within and across domains.
Record (noun)	Information in any format created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business.
Record category	A subdivision of the records classification scheme, which may be further subdivided into one or more lower-level record categories. NOTE 1 A record category is constituted of metadata which may be inherited from the parent and passed on to a child. NOTE 2 The full set of record categories, at all levels, together constitutes the records classification scheme.
Records management	The field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of, and information about, business activities and transactions in the form of records.
Records management metadata	Data that identifies authenticates and contextualises records and the people, processes and systems that create, manage, maintain and use them, and the policies that govern them.

Term	Definition
Records management system	A framework to capture, maintain and provide access to evidence over time, as required by the jurisdiction in which it is implemented and in accordance with common business practices. NOTE 1 Records management systems include both records practitioners and records users; a set of authorised policies, assigned responsibilities, delegations of authority, procedures and practices; policy statements, procedures manuals, user guidelines and other documents which are used to authorise and promulgate the policies, procedures and practices; the records themselves; specialised information and records systems used to control the records; and software, hardware and other equipment, and stationery.
Redaction	The process of masking or deleting information in a record.
System administrator	A user role with designated responsibility for configuring, monitoring and managing the business system and its use.
Thesaurus	A records classification tool comprising an alphabetical presentation of a controlled list of terms linked together by semantic, hierarchical, associative or equivalence relationships. NOTE 1 In a thesaurus, the meaning of a term is specified and relationships to other terms are shown. A thesaurus should provide sufficient entry points to allow users to navigate from non-preferred terms to preferred terms adopted by the organisation.
Taxonomy	The classification of entities in an ordered system that indicates natural relationships.
Tracking	Creating, capturing and maintaining information about the movement and use of records.
Transaction	1 The smallest unit of business activity. Uses of records are themselves transactions. NOTE 1 The third or lowest level in a business classification scheme.

Term	Definition
Transfer	A disposition process consisting of an export of digital records and associated metadata to another system, application organisation or agent, NOTE 1 Records may be transferred from one organisation to another following administrative change, from an organisation to archival custody, from an organisation to a service provider, from the government to the private sector or from one government to another.
Volume	A sub-division of a digital or non-digital aggregation. NOTE 1 Also referred to as a 'part'. NOTE 2 A volume is usually a file part closed off due to size or time period constraints, for example, 'Expense claim forms 2007–2008'.

4. GUIDELINES

4.1 Why implement a digital records management system?

4.1.1 What are record attributes?

A record is not just a collection of data, but is the consequence or product of an event, business action or transaction, and therefore inextricably linked to business activities. A distinguishing feature of records is that their content exists in a fixed form, that is, a fixed representation of the business transaction. Records comprise not only the informational content but also information about the context and structure of the record. ISO 15489-1:2001, *Information and documentation — Records management — Part 1: General* sets out the key attributes of a record and the high level considerations and processes for managing records effectively and should be a key reference document for implementing this part. The essential records attributes can be summarised as;

a) **Authenticity** – the record can be proven to be what it purports to be, to have been created or sent by the person that created or sent it, and to have been created or sent at the time it is purported to have occurred.

b) **Reliability** – the record can be trusted as a full and accurate representation of the transaction(s) to which they attest, and can be depended on in the course of subsequent transactions.

c) **Integrity** – the record is complete and unaltered, and is fixed. This characteristic is also referred to as ‘inviolability’.

d) **Usability** – the record can be located, retrieved, preserved and interpreted.

To maintain these records attributes effectively and reliably over time it is necessary to implement a digital records management system.

4.1.2 What are digital records management system attributes?

The use of the term ’system’ in this document refers to a collection of computer hardware and/or software and includes plug-ins or other Information Technology system components. This is in contrast to the records management understanding of the term, which encompasses the broader aspects of people, policies, procedures and practices that combine to form an overall systematic approach. While the focus of this part is primarily digital records management systems software applications, organisations will need to pay attention to the wider aspects of records management frameworks, policies and tools to ensure records can be appropriately managed. For example, for a digital records management system to function effectively, fundamental records management tools, such as disposition authorities and information security classifications, have to be in place and operate within an established records management culture within an organisation.

Typically, digital records management systems have the following attributes that seek to ensure that key records characteristics are maintained:

a) creating and capturing records in context

b) managing and maintaining records controls

c) maintaining records for as long as they are required

d) implementing records disposition.

e) the management of records management metadata.

4.1.3 Risks and benefits of implementing digital records management systems

4.1.3.1 Risks of not implementing digital records management systems

The risks of not implementing a digital records management system include:

- failure to meet legislative and regulatory requirements;
- embarrassment to your chief executive, brand, organisation, the government and/or private individuals, especially if inability to manage information competently is highlighted in the news media;
- poor strategic planning and poor decisions based on inaccurate information;
- business critical information not accessible for the conduct of business, dispute resolution, legal challenge or evidential purposes;
- loss of credibility, lowered public confidence, or financial or legislative penalties through inability to produce records or provide evidence of business activity when required in a timely manner;
- inability to provide evidence of the organisation's activities or undertakings with external organisations, clients or contractors;
- inconsistent and inefficient conduct of business;
- inability to exploit organisational information and knowledge to full potential;
- unlawful disposition of records and inability to fully exploit corporate knowledge and data;
- duplication of effort, and poor resource and asset management;
- reduced capability of demonstrating good performance and any increased efficiencies or improved service delivery; and
- organisational embarrassment and damage to reputation.

4.1.3.2 Benefits of implementing digital records management systems

The benefits of implementing digital records management systems include:

- protection and support in litigation, including the management of risks associated with the existence or lack of evidence of organisational activity;
- protection of the interests of the organisation and the rights of employees, clients, and present and future stakeholders;

- improved security of business records and robust management of commercial-in-confidence, personally sensitive or confidential information;
- the ability to deliver services in an efficient and consistent manner;
- ability to support current and future research and development activities;
- improved comprehensiveness and reliability of corporate memory;
- availability of relevant business activity records when required to support well-informed decision-making and policy development;
- reduced risk of data loss or accidental destruction of records;
- reliable performance measurement of business outputs;
- increased public and/or client confidence in the integrity of an organisation's activities; and
- identification of vital records for disaster planning, so that organisations can continue to function in the event of severe disruption.

4.2 Overview of functional requirements

4.2.1 Structure of functional requirements

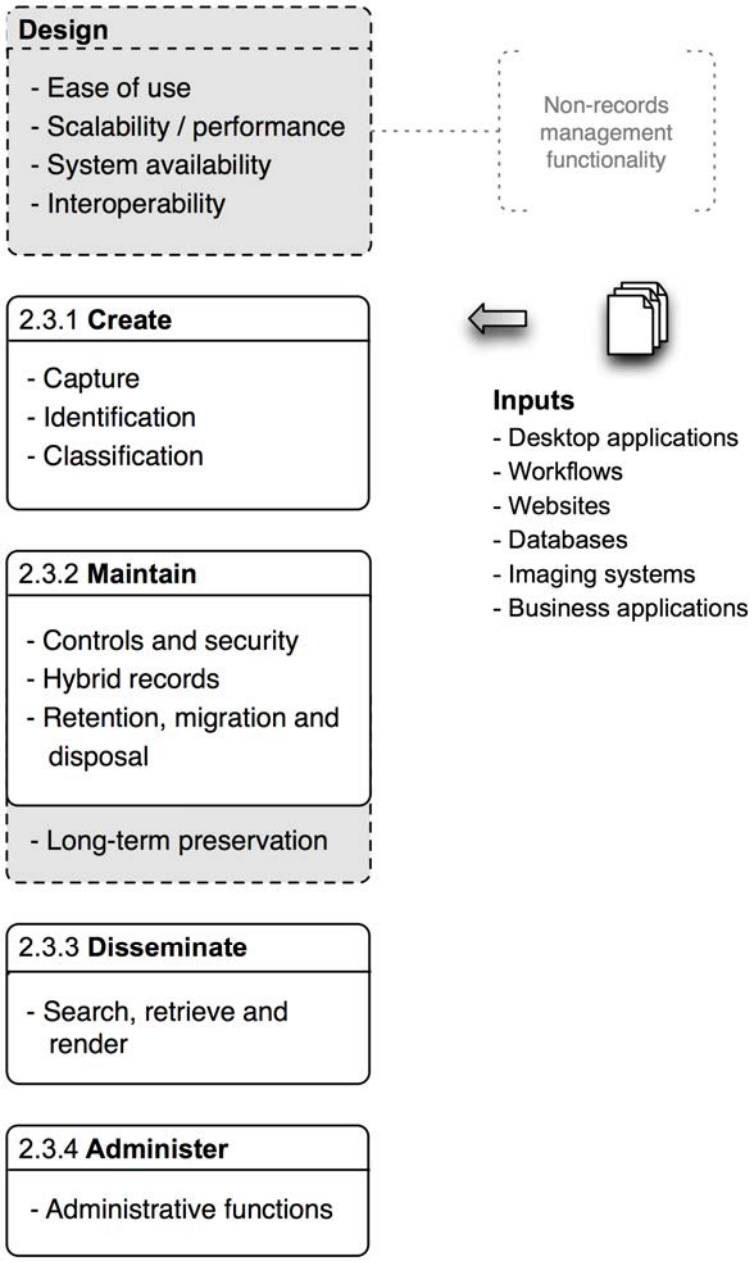
This section identifies and briefly describes the functional requirements using a high-level model that clusters the requirements to highlight their inter-relationships (Figure 1).

Requirements for the long-term preservation of records, requirements common to all software applications and non-records management functionality are not detailed in this part, but are indicated in the high-level model (solid grey shading). Potential integration points with IT architecture and other software applications are shown in the model as system inputs.

Individual requirements in *Part 5: Functional requirements* are grouped according to the clusters in the high-level model:

1. create
2. maintain
3. disseminate
4. administer.

Figure 1: Model of high-level functional requirements for digital records management systems



NOTE 1 Solid grey shading indicates functionality not detailed in *Part 5: Functional requirements*.

NOTE 2 This model depicts the functional requirements that are the components of digital records management systems. It does not depict the sequence of work processes that digital records management systems perform.

4.3 Guidance for implementing high-level functional requirements

4.3.1 Create

4.3.1.1 Capture

Digital records management systems uniquely capture, classify and identify records to ensure that their content, structure and context of creation are fixed in time and space. They also provide the functionality to create a new record by reusing the content, structure and context of records once captured. While version/document control is beyond the scope of this part it may be useful to bundle this functionality into a digital records management system.

4.3.1.2 Records management metadata

Records management metadata is an essential component of records management, serving a variety of functions and purposes. In a records management context, metadata is defined as data describing the context, content and structure of records and their management through time. As such, metadata is structured or semi-structured information that enables the creation, registration, classification, access, preservation and disposition of records through time and within and across domains.

Records management metadata can be used to identify, authenticate and contextualise records and the people, processes and systems that create, manage, maintain and use them, and the policies that govern them. Initially, metadata defines the record at its point of capture, fixing the record into its business context and establishing management control over it. For the duration of a records' or record aggregations' retention, new layers of metadata will be added because of new actions or uses for the content in other business or usage contexts. This means that metadata continues to accrue information relating to the context of the records management and the business processes in which the records are used and to structural changes to the record or its appearance.

Metadata can be sourced from, or re-used by, multiple systems and for multiple purposes. Metadata applied to records during their active life may also continue to apply when the records cease to be required for current business purposes but are retained for ongoing research or other values. The purpose of records management metadata is to ensure authenticity, reliability, usability and integrity over time, and to enable the management and understanding of information objects, whether these are physical, analogue or digital. However, metadata also needs to be managed as a record or as the component of a record.

Records management has always involved the management of metadata. However, the digital environment requires a different expression of these traditional requirements and different mechanisms for identifying, capturing, attributing and using metadata. In the digital environment, authoritative records are those accompanied by metadata defining their critical characteristics. These characteristics shall be explicitly documented rather than being implicit, as is common in some paper-based processes.

ISO 23081-2:2009, *Information and documentation — Managing metadata for records — Part 2: Conceptual and implementation issues* provides a generic

statement of records management metadata elements and should be used as a key reference document for implementing the functional requirements. Organisations may also have jurisdiction-specific elements sets to which they shall adhere.

4.3.1.3 Records aggregations

Aggregations of digital records are accumulations of related digital record entities that, when combined, may exist at a level above that of a singular digital record object, for example, a file. Aggregations represent relationships that exist between related digital records and the system or environment in which they were created and these relationships are recorded within their metadata links and/or other associations. These aggregations are typically controlled within a classification scheme in a digital records management system.

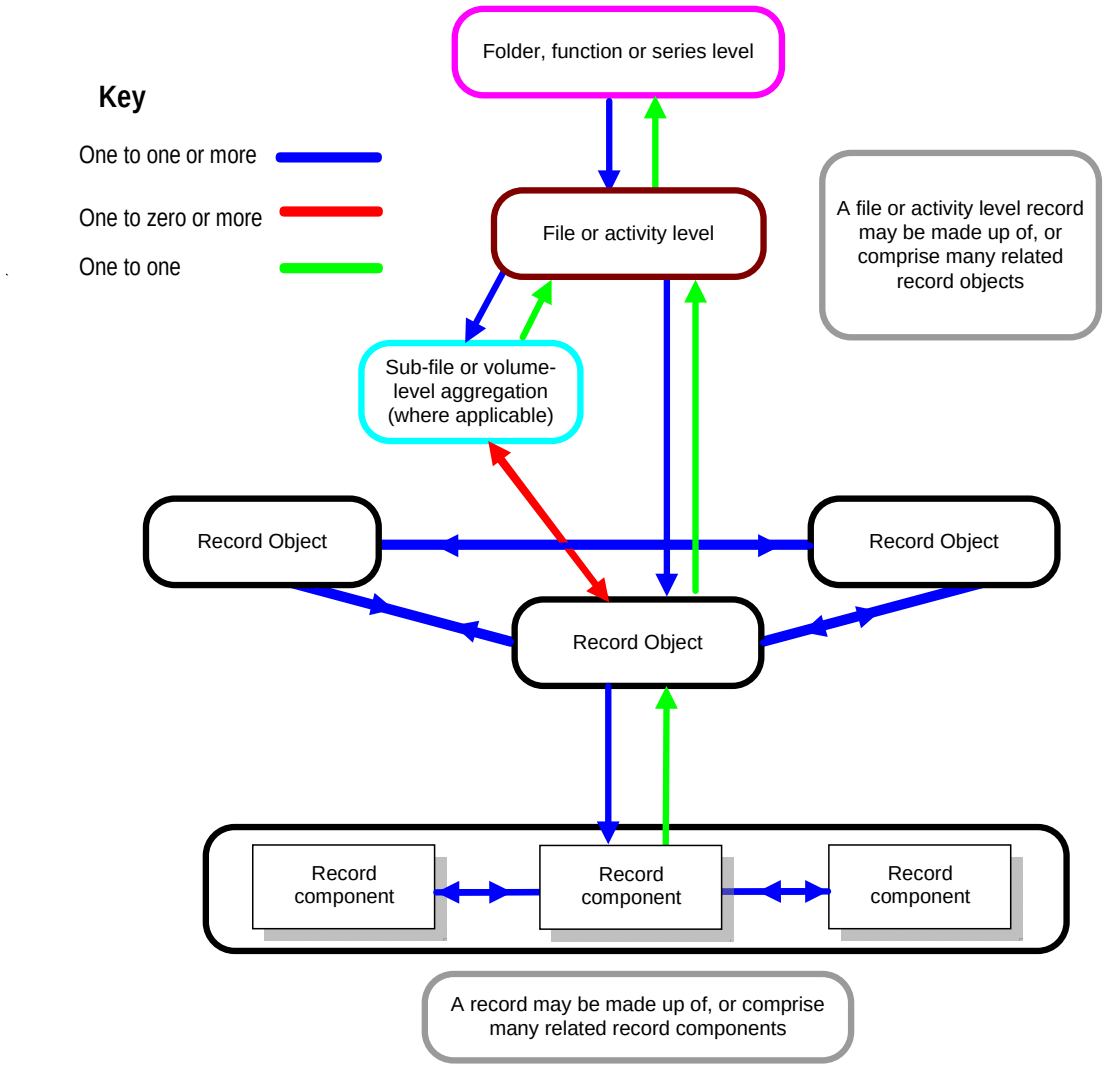
Aggregations of digital records may reflect relationships such as shared characteristics or attributes, or the existence of sequential relationships between related digital records. The nature of the relationship between the digital records of a particular aggregation will vary depending on factors such as their purpose and structure, and the content and format of the records themselves. Records aggregations may be at more than one level, and may have multiple relationships within separate aggregations.

For example, an aggregation of digital records may collectively constitute a narrative of events (that is, a series of connected business transactions), in which the records may have a sequential relationship. Any such sequential relationship between digital records can be determined through the metadata elements associated with the records, such as titles, dates, author, container number (where applicable), and other such attributes. Where these relationships exist between records imported or extracted from external business systems, the digital records management system shall be capable of identifying, capturing, documenting and preserving them.

These aggregations may be formal, structured relationships (for example, digital files containing related digital documents), or may exist as less formalised metadata relationships recognised as establishing links between related records within an aggregation.

The aggregations shall be fixed and maintained over time. Any change to an aggregation shall be logged with an explanation. Aggregation for the management of records purposes should not be confused with, or replaced by, the generation of multiple, different aggregations in response to search requests or report queries.

Figure 2: Aggregation of records



4.3.1.4 Supporting import, export and interoperability

The ability to import and export records, and interoperability with other systems or newer versions of the existing digital records management system, is a core set of required functionality. Records may need to be exported to other organisations, other systems or for internal or internal archival storage.

Many records may need to be retained for longer than the lifespan of the software or system itself, and therefore there is a need to be able to export records when transitioning to a new digital records management system. There may also be a need to import records from business systems, particularly in collaborative business environments.

For ease of import and export, use of open formats and industry standards will increase levels of interoperability and reduce the cost and difficulty of any import/export process.

This functionality shall be addressed at the planning stages as part of the business requirements.

4.3.1.5 Identification - unique identifiers

To verify their existence within the system, every record and associated aggregation shall have a unique identifier persistently linked to it. This allows the user to locate records and helps them to distinguish between versions.

4.3.1.6 Classification

Within digital records management systems implementations, aggregations are often used to enable inheritance of characteristics to records created or related at a lower level of aggregation. Typically in digital records management systems, information is managed as a collection of record objects, and aggregates these objects into a set of series or folders or files. Organisations should take into account their own business needs when determining suitable records aggregations (for example, by function, activity or transaction) within their organisation. Within a business classification scheme, a record's contextual characteristics are attributed through structuring them according to identifiable business processes.

Subject-based classification schemes will allow records relating to broad subject areas to be grouped together, that is, the transactions and activities that occurred under a single subject, such as a particular property or client. However, under subject-based classification, the focus is on what the item or object is about, rather than on the purpose or activity that the record was created to document. Therefore, the context of the business activity can become disassociated, making disposition actions over subject-based files more difficult as they will contain records with differing retention periods.

Functional classification schemes are based on an analysis of the unique business functions and activities of an organisation, and are independent of the organisation's administrative structure. This makes functional classification more flexible and stable as business units and structures are likely to change over time. This system breaks down traditional organisational information silos and enables easier retention and disposition.

4.3.1.7 Business classification schemes

A business classification scheme is a conceptual hierarchical classification tool that facilitates the capture, titling, retrieval, maintenance and disposition of records. It defines the way in which records are grouped together (aggregated) and linked to the business context in which they were created or transmitted. For example, individual records in an organisation-wide digital records management system may be aggregated into series with their constituent record parts and contextual metadata, or may be subsequently aggregated into files or folders. Records are often aggregated at three levels of granularity according to a three-tiered functional classification scheme as follows:

Figure 3: Three-tiered functional classification scheme

Level 1	**Business function**
Highest level (Series), consisting of aggregations of files, may be referred to as ‘class’ or ‘category’	
Level 2	**Activity**
Files, consisting of aggregations of individual records, may be referred to as ‘folders’ or ‘containers’. May be subdivided into volumes.	
Level 3	**Transaction**
Items – in this document referred to as ‘records’. May be comprised of multiple components.	

NOTE 1 This is a basic model. Aggregation to more than three levels may be necessary depending on the business processes described, or for clearer definition of complex topics.

NOTE 2 The record (object) is located at the very bottom of the aggregation hierarchy for the purposes of classification although the record object may comprise multiple related components. Some metadata values may be inherited from a higher layer of aggregation by all those files or objects located below.

NOTE 3 Regardless of how many levels of aggregation below series or file level are implemented; each level should be consistent with the metadata requirements for the higher aggregation level.

4.3.2 Maintain

4.3.2.1 Managing authentic and reliable records

Records captured into digital records management systems shall be actively maintained to ensure their continued accessibility. Establishing appropriate security controls, building in disposition outcomes and enabling the management of hybrid records facilitate comprehensive, authentic, useable, tamper-proof and appropriate records management.

4.3.2.2 Controls and security

Records captured into a digital records management system shall be protected against intentional or accidental alteration of their content, structure and context throughout their life to retain their authenticity. Digital records management systems shall control access to, or alteration of, metadata. Location tracking, access controls and control over any alteration of records ensure the authenticity of records in a digital records management system. The digital records management system should automatically alert an administrator that an alteration has occurred and have enough redundancy in backups that a correct version can be recovered.

4.3.2.3 Authentication, encryption and technological protection measures

The application of authentication, encryption and digital rights management issues can have a significant impact on the reliability of records. Digital records management systems shall allow records to be effectively managed when they have been subject to technological protection measures, digital signatures and digital watermarks or other digital rights management protocols. System administrators should give particular consideration to the ongoing maintenance of records that have been subject to encryption and/or other digital rights management processes.

While encryption and digital signatures have a valuable role to play in ensuring the authenticity and integrity of records in transmission, they also present risks to the ongoing useability of the record as decryption keys and public keys for digital signatures may expire while the record is still required. For this reason, storing records in encrypted form is not recommended. Metadata can be applied to record the encryption and decryption processes and attest to the successful decryption of records.

If digital signatures are used as a means of protecting the authenticity and integrity of records, key management shall be considered. Information about the digital signature and its validation should be recorded within the metadata.

4.3.2.4 Hybrid records management

Organisations typically manage records that span a range of digital and non-digital media. Digital records management systems shall be able to ingest and maintain records management metadata relating to non-digital records as well as digital records and any associated records management metadata. Essentially, contextually related records regardless of whether they are in digital or non-digital format shall be managed and subject to the same records management processes within their aggregations.

To facilitate hybrid records management functionality, the digital records management system shall be able to capture and maintain metadata relating to physical records. This requires the creation of markers, which are metadata profiles of records physically held outside the business system. Markers contain metadata required by the business system to locate and manage physical records and allocate system management controls to them. A marker may denote a physical record, such as a plan or paper file, or a digital record or aggregation of digital records stored on removable media, such as an eternal hard drive, CD-ROM, magnetic tape or microform.

4.3.2.5 Retention and disposition

Disposition authorities are policies that authorise the disposition of records, whether by destruction, transfer of control, applying a review period or other disposition actions. Disposition authorities consist of disposition actions and retention periods for aggregations of records that may have a legislative or organisational source. Organisations should review disposition actions when the relevant retention periods have expired rather than automate the destruction of records.

Records are often transferred between digital records management systems for a range of reasons other than disposition, for example, migration to a new digital

records management system as a result of a technology refresh or an organisational restructure. In all cases, where there is transfer of records (whether this involves movement to another digital records management system or not) and/or subsequent destruction of records from the original digital records management system, any existing records management metadata and point of capture metadata shall be considered at the same time as the records to which they relate.

4.3.3 Disseminate

A digital records management system shall be able to search for, retrieve and render the records that it maintains. These functions facilitate useable records.

4.3.3.1 Search

Searching is the process of identifying records or aggregations through user-defined parameters so that the records, aggregations and/or their associated records management metadata can be retrieved. Search and navigation tools are required to locate records, or records aggregations or records management metadata by employing a range of searching techniques to cater for both novice and sophisticated users. Retrieving is the process of preparing the located records for rendering and viewing.

4.3.3.2 Render

Rendering is the (re)production of a human-readable representation of a record, usually to a visual display screen or in hardcopy format. Digital records management systems typically contain records in a range of file formats. The user shall be able to have human-readable access to records stored in all formats through an appropriate rendering interface. Where it is meaningful to print a hardcopy of a record, the digital records management system shall provide functionality to allow all users to obtain printed copies of records and their records management metadata where appropriate.

4.3.4 Administer

As with most software applications, there is a need for a system administrator to undertake system maintenance and other support functions, such as maintenance of access groups and updating of the business classification system. This part only refers to system administration in the sense of the digital records management functionality and the routine application of records management procedures. The following table sets out an example of administrator/user roles.

Table 1: System levels of access

User	Any person with permission to access the digital records management system. That is, anyone who creates, receives, reviews and/or uses records stored in the system. This is the standard level of access that most employees of an organisation will possess.
Authorised user	A user with special access permissions that allow additional access to, and/or control over, records contained in the digital records management system. Authorised users may in some instances be assigned permissions to undertake tasks similar to those of the system administrator, such as the ability to close and re-open records, create extracts of records and edit record metadata. The powers assigned to authorised users will vary depending on the business needs of the organisation and the level of responsibility allotted to the authorised user.
Records administrator (or records manager)	A system administrator, usually the records manager, with designated responsibility for configuring, monitoring and managing the digital records management system content and its use.
System administrator (IT)	A person with responsibility for assigning and removing the permissions allocated to users and authorised users.

5. FUNCTIONAL REQUIRMENTS

This section sets out the set of functional requirements for digital records management systems. They are divided into four sections according to key records management concepts and processes as outlined in *Part 4: Guidelines*:

5.1. create

5.2. maintain

5.3. disseminate

5.4. administer.

The functional requirements are focused on the outcomes required to ensure records are managed appropriately. They do not specify particular processes, as it is recognised that the techniques and strategies to achieve these outcomes will depend on the organisation and digital records management system being used. The introductory text to each section provides summary information regarding the records management concept and the overarching aim of the subsequent requirements.

While they do not cover general requirements common to the system management and design of all systems and applications, such as interoperability, scalability and performance, it is acknowledged that such processes also support the records management functionality of the digital records management system. The functional requirements assume that a basic records management framework is in place, such as policies, procedures, and business retention and classification.

The functional requirements focus on the outcomes required to ensure records are managed appropriately, regardless of the type of digital records management system employed. As the functional requirements provide a high-level description of records management functionality rather than detailed specifications, it is recognised that the techniques and strategies to achieve the outcomes will depend on the type of system being used. It is intended that each organisation should tailor the functional requirements to meet its individual business needs.

Risk is an important factor that should be considered in the management of records and applying these obligation levels and requirements. Possible risks may include adverse publicity, inefficient business activity, impaired ability to deliver services and a reduction in the organisation’s capacity to prosecute or defend allegations.

There is a wide range of requirements to show evidence of business processes. If there are any requirements that an organisation is considering not meeting, a risk and feasibility analysis can help determine an appropriate course of action, and ensure accountability in decision-making.

Organisations may have jurisdiction-specific risk management frameworks in place that define different levels of risk, which can be used to prioritise the identified requirements for evidence. A feasibility analysis can help organisations to consider, in a structured way, the financial, technical, legal or operational capacity of the organisation.

5.1 CREATE

5.1.1 Capture

Records are created in a diverse range of formats, may comprise multiple individual objects (compound records), and are transmitted by a wide range of communication channels (workflows, email, postal mail). Digital records management systems shall capture the content, structure and context of records to ensure they are reliable and authentic representations of the business activities or transactions in which they were created or transmitted. This is known as 'point of capture' metadata and should in itself be captured as a record; it should not be possible to alter any of these metadata features without changes being tracked and auditable.

5.1.2 Capture processes

The digital records management system **shall**:

1	Enable integration with business applications so that transactional records created by those applications can be captured within the digital records management system (including email, see Requirements 21–25).
2	Indicate when an individual record is captured within the digital records management system.
3	Prevent the alteration of the content of any record by any user or administrator during the process of records capture (see also Requirements 88 and 89).
4	Prevent the destruction or deletion of any record by any user, including an administrator, with the exceptions of: 1. destruction in accordance with a disposition authority (see Section 5.6: Retention and disposition); and 2. authorised deletion by an administrator (see Section 5.8: Administration).
5	Support manual naming of digital records, and allow this name to be different from the existing file name (including email subject lines used to construct record titles). If the existing filename is taken by default, the digital records management system shall allow this name to be amended at the time of capture.
6	Allow an administrator to alter the metadata of a record within the system if required, to allow finalisation/correction of the record profile. Any such action shall be captured in a records management metadata.
7	Any revision or alteration of the records management/capture metadata shall be captured as additional records management metadata.
8	Alert a user to any failure to successfully capture a record.
9	Be able, where possible and appropriate, to provide a warning if an attempt is made to capture a record that is incomplete or inconsistent in a way which will compromise its future apparent authenticity.

5.1.3 Point of capture metadata

To be meaningful as evidence of a business process, records shall be linked to the context of their creation and use. In order to do this, the record shall be associated with metadata about the business context in which it was created and its point of capture into the system

Much of this information can be automatically generated by the system and user attributed metadata should be minimised for ease of creation and to avoid human error. It is expected that each organisation will capture records management metadata in line with an identified records management metadata standard (compliant with the ISO 23081 series standards), and any organisational and/or legislative requirements.

The digital records management system **shall**:

10	Support the use of persistent metadata for records.
11	Acquire metadata elements for each record and persistently link them to the record over time.
12	Ensure that the values for metadata elements conform to specified encoding schemes.
13	Allow the administrator to pre-define (and re-define) the metadata elements associated with each record, including whether each element is mandatory or optional.
14	Allow all metadata for every record to be viewed by users, subject to access rights for individuals or groups of users.
15	Automatically capture the date and time of capture of each record as metadata elements linked to each record.
16	Support automatic extraction or migration of metadata from: 1. the software application that created the record; 2. an operating system or line of business system; 3. a digital records management system; and 4. the file header, including file format metadata, of each record and its constituent components captured into the system.
17	Prevent the alteration of metadata captured in Requirement 16, unless authorised by the system administrator.
18	Allow entry of additional metadata by users during record capture and/or a later stage of processing by the user.
19	Ensure that only authorised users and administrators can change the content of records management metadata elements.
20	Allocate an identifier, unique within the system, to each record at point of capture automatically.

5.1.4 Aggregation of digital records

Where metadata elements associated with identifying and maintaining aggregation relationships, such as titles, dates, author, container number (where applicable), and other attributes exist, the system shall be capable of identifying, capturing, documenting and maintaining or systematically disposing of them.

The digital records management system **shall**:

21	Ensure that all records captured within the digital records management system are associated with at least one aggregation.
22	Manage the integrity of all markers or other reference tags to records (where used), ensuring that: 1. following a marker, whichever aggregation that the marker record is located in, will always result in correct retrieval of the record; and 2. any change in location of a record also redirects any marker that references that record.
23	Not impose any practical limit on the number of records that can be captured in an aggregation, or on the number of records that can be stored in the digital records management system. However, the system may permit the administrator to set limitations on the quantity of items within an aggregation if required for business purposes.

24	Allow users to choose at least one of the following where a digital object has more than one manifestation: 1. register all manifestations of the object as one record; 2. register one manifestation of the object as a record; or 3. register each manifestation of the object as a discrete record.

The digital records management system **should**:

25	Support the ability to assign records to multiple aggregations without their duplication.[1]

5.1.5 Bulk importing

Records and their metadata may be captured into a digital records management system in bulk in a number of ways, for example, from another digital records management system or as a bulk transfer from a digital document management system or workflow application. The digital records management system shall be able to accept these, and shall include features to manage the bulk capture process.

The digital records management system **shall**:

[1] For example, an invoice might be added to a supplier file by one user and to a product file by another. This could be achieved by using a marker system.

26	Be able to capture in bulk records exported from other systems, including capture of: 1. digital records in their existing format, without degradation of content or structure, retaining any contextual relationships between the components of any individual record; 2. digital records and all associated records management metadata, retaining the correct contextual relationships between individual records and their metadata attributes; and 3. the structure of aggregations to which the records are assigned, and all associated records management metadata, retaining the correct relationship between records and aggregations.[2]
27	Be able to import any directly associated event history metadata with the record and/or aggregation, retaining this securely within the imported structure.

5.1.6 Digital document formats

Digital records management systems will have to deal with a wide range of formats, both common applications and often business-specific formats. The digital records management system shall have the functionality to deal with the formats that the organisation commonly uses or are common to the relevant business environment. This will vary across systems and organisations.

For ease of migration and export, use of open formats and industry standards will increase levels of interoperability and reduce the cost and difficulty of maintaining records effectively.

The digital records management system **shall**:

28	Support the capture of records created in native file formats from commonly used software applications such as: 1. standard office applications (word processing, spread-sheeting, presentation, simple databases); 2. email client applications; 3. imaging applications; and 4. web authoring tools.
29	Be able to extend the range of file formats supported as new file formats are introduced for business purposes or for archival retention (for example, PDF/A).[3]

[2] For example, maintaining a persistent embedded metadata record of the original classification schema.

[3] It is not always possible to capture specialised records (or those from specialised systems) with a digital records management system; however, this risk should be mitigated against. Strategies for normalisation of formats for capture or a process of capturing the entire system should be considered. Where this is not possible, building records management capability into the business information system should be considered.

5.1.7 Compound records

Digital records will comprise at least one component. Digital records such as a text document will usually be a discrete record and comprise a single record object. Digital records that comprise more than one component or multiple record objects, for example, a large technical report with dynamic links to diagrams and spreadsheets, may be referred to as a compound record.

The nature of the components that comprise a given digital record will vary. A component may be a digital object, such as a digital document, or a data element, such as a cell, or row, in a database. For example, in a document management system a record may consist of a single word-processed text box, table or image within a document, while components forming a digital record in a human resource management spreadsheet may comprise a number of closely linked data entries in a database (such as all data entered in connection with a single staff member's personnel profile).

The digital records management system **shall**:

30	Capture compound digital records (records comprising more than one component) so that: 1. the relationship between the constituent components of each compound record is retained; 2. the structural integrity of each compound record is retained; and 3. each compound record is retrieved, displayed and managed as a single unit.
31	Be able to capture compound records easily, preferably with one action, for example, a single click.

5.1.8 Email

Email is used for sending both simple messages and documents (as attachments), within and between organisations. The characteristics of email can make it difficult to track and register. Organisations shall provide users with the capability of capturing selected email messages and attachments.

The digital records management system **shall**:

32	Allow users to capture emails (text and attachments) as single records as well as individual records linked by metadata.
33	Allow individual users to capture email messages (and attachments) from within their email application.
34	Allow users to choose whether to capture emails with attachments as: 1. email text only; 2. email text with attachments; or 3. attachments only.[4]

[4] It is essential that these processes are recorded and embedded within the metadata of the records. The user shall be alerted to the existence of the related items.

35	Ensure the capture of email transmission data as metadata persistently linked to the email record.
36	Ensure that the text of an email and its transmission details cannot be amended in any way once the email has been captured. Nor should the subject line of the email itself be changeable, although the title of the record may be edited for easier access through, for example, keywords or by file-naming conventions.
37	Ensure that a human-readable version of an email message address is also captured, where one exists.[5]

5 For example, for ‘Samuel Johnson’ <samjo@worldintnet.org> – ‘Samuel Johnson’ is the human-readable version of the email address samjo@worldintnet.org.

5.2 Identification

To verify the existence of a record within a system, every record and associated aggregation shall have a unique identifier persistently linked to it. This allows to the user to locate records and helps them to distinguish between versions.

The digital records management system **shall**:

38	Associate each of the following with a unique identifier: 1. record; 2. record extract; and 3. aggregation.
39	Require all identifiers to be unique and unduplicated within the entire digital records management system.
40	Be able to store the unique identifiers as metadata elements of the entities to which they refer.
41	***Either*:** Generate unique identifiers automatically, and prevent users from inputting the unique identifier manually and from subsequently modifying it (for example, a sequential number).
42	***Or*:** Allow users to input a unique identifier, but validate that it is unique before it is accepted (for example, an account number).
43	Allow the format of the unique identifier to be specified at configuration time.[6]

Where unique identifiers are automatically generated, the digital records management system **should**:

44	Allow the administrator to specify at configuration time the starting number (for example, 1, 10, 100) and increment (for example, 1, 10) to be used in all cases.

6 The identifier may be numeric or alphanumeric, or may include the concatenated identifiers of the volume and digital aggregations above the record in the classification scheme.

5.3 Classification

5.3.1 Establishing a classification schemes

A records classification scheme is a hierarchical classification tool that can facilitate the capture, titling, retrieval, maintenance and disposition of records. A classification scheme lies at the heart of any digital records management system since it defines the way in which individual digital records are grouped together (aggregated) and linked to the business context in which they were created or transmitted. Where a pre-exisiting classification scheme or system is not available, it will be necessary to create one.

NOTE 1 A classification scheme/system may also be manifested as a metadata framework as well as an externally designed or applied structure.

The digital records management system **shall**:

45	Support and be compatible with the organisational classification scheme.
46	Be able to support a classification scheme that can represent aggregations (at the function, activity, transaction level) as being organised in a hierarchy with a **minimum** of three levels.
47	Allow the inheritance of values from a classification scheme.
48	Allow naming conventions or thesauri to be defined at the time the digital records management system is configured.
49	Support the initial and ongoing construction of a classification scheme.
50	Allow administrators to create new aggregations at any level within any existing aggregation.
51	Not limit the number of levels in the classification scheme hierarchy unless set by an administrator.
52	Support the definition of different record types that are associated with a specified set of metadata to be applied at capture.
53	Support the allocation of unique identifiers to records within the classification structure

Where the unique identifiers are based on sequential numbering, the digital records management system **should**:

54	Have the capacity to automatically generate the next sequential number within the classification scheme for each new digital aggregation.[7]

7 For example, if the following aggregations are within a classification scheme:

• 900 - 23 - 01 Manufacturing : Order Processing : Sales Order Validation;

• 900 - 23 - 02 Manufacturing : Order Processing : Invoicing;

• 900 - 23 - 03 Manufacturing : Order Processing : Credit Note Processing;

and the administrator adds a new aggregation to the ‘Order Processing’ aggregation, the digital records management system should automatically assign it the reference 900 - 23 - 04. Likewise, if the

The digital records management system **may**:

55	Support a distributed classification scheme that can be maintained across a network of digital record repositories.

Where the digital records management system employs a graphical user interface, it **shall**:

56	Support browsing and graphical navigation of the aggregations and classification scheme structure, and the selection, retrieval and display of digital aggregations and their contents through this mechanism.

The digital records management system **should**:

57	Support the definition and simultaneous use of multiple classification schemes. This may be required, for example, following the merger of two organisations or migration of legacy systems. It is not intended for routine use.

5.3.2 Classification levels

The digital records management system **shall**:

58	Support metadata for levels within the classification scheme.
59	Provide at least two naming mechanisms for records in the classification scheme: 1. a mechanism for allocating a structured alpha, numeric or alphanumeric reference code (that is, an identifier which is unique within the classification scheme) to each classification level; and 2. a mechanism to allocate a textual title for each digital aggregation. 3. It shall be possible to apply both identifiers separately or together.
60	Allow only authorised users to create new classifications at the highest level in the classification scheme (for example, at the business function level).
61	Record the date of opening of a new aggregation within its associated records management metadata.
62	Automatically include in the records management metadata of each new aggregation those attributes that derive from its position in the classification scheme (for example, name, classification code).[8]
63	Allow the automatic creation and maintenance of a list of classification levels.

administrator adds a new class to the 'Manufacturing' aggregation, the digital records management system should automatically assign it the reference 900 - 24.

8 For example, if a file is in a hierarchical path: 'Regional plan development : Public consultation : Public submissions' and the administrator adds a new file named 'Formal objections' at the same level as the 'Public submissions' file, then it shall automatically inherit the prefix 'Regional plan development : Public consultation'.

The digital records management system **should**:

64	Support a naming mechanism that is based on controlled vocabulary terms and relationships drawn (where appropriate) from an ISO 2788-compliant or ISO 5964-compliant thesaurus and support the linking of the thesaurus to the classification scheme.
65	Support an optional aggregation naming mechanism that includes names (for example, people's names) and/or dates (for example, dates of birth) as file names, including validation of the names against a list.
66	Support the allocation of controlled vocabulary terms compliant with ISO 2788 or ISO 5964 as records management metadata, in addition to the other requirements in this section.

5.3.3 Classification processes

The digital records management system **shall**:

67	Allow a digital aggregation (including volumes) to be relocated to a different position in the classification scheme, and ensure that all digital records already allocated remain allocated to the aggregations (including volumes) being relocated.[9]
68	Allow a digital record to be reclassified to a different volume of a digital aggregation.[10]
69	Restrict to authorised users the ability to move aggregations (including volumes) and individual records.
70	Keep a clear history of the location of reclassified aggregations (including volumes) prior to their reclassification, so that their entire history can be determined easily.[11]
71	Prevent the deletion of a digital aggregation or any part of its contents at all times, with the exceptions of: 1. destruction in accordance with a disposition authority; and 2. deletion by an administrator as part of an audited procedure.
72	Allow a digital aggregation to be closed by a specific administrator procedure, and restrict this function to an administrator.
73	Record the date of closing of a volume in the volume's records management metadata.

9 This facility is intended for exceptional circumstances only, such as organisational mergers or other re-organisation, or to correct clerical errors. This requirement shall be read together with Requirements 71, 72 and 80.

10 This facility is intended for exceptional circumstances only, such as to correct clerical errors. This requirement shall be read together with Requirements 71, 72 and 80.

11 At a minimum, this shall be stored in the metadata. It may also be desirable to record it elsewhere, for example, in the records management metadata of the object(s) being moved.

74	Maintain internal integrity (relational integrity or otherwise) at all times, regardless of: 1. maintenance activities; 2. other user actions; and 3. failure of system components.[12]
75	Not allow any volume that has been temporarily re-opened to remain open after the administrator who opened it has logged off.
76	Allow users to create cross-references between related aggregations or between aggregations and individual records.
77	Provide reporting tools for the provision of statistics to the administrator on aspects of activity using the classification scheme, including the numbers of digital aggregations (including volumes) or records created, closed or deleted within a given period, by user group or functional role.
78	Allow the authorised users to enter the reason for the reclassification of aggregations (including volumes) and individual records.
79	Be able to close a volume of a digital aggregation automatically on fulfilment of specified criteria to be defined at configuration, including at least: 1. volumes delineated by an annual cut-off date (for example, end of the calendar year, financial year or other defined annual cycle); 2. the passage of time since a specified event (for example, the most recent addition of a digital record to that volume); and 3. the number of digital records within a volume.[13]
80	Be able to open a new volume of a digital aggregation automatically on fulfilment of specified criteria to be defined at configuration.
81	Allow an administrator to lock or freeze aggregations to prevent relocation, deletion, closure or modification when circumstances require, for example, pending legal action.

5.3.4 Record volumes

This section includes requirements relating to the use of volumes, which are typically used to subdivide aggregations that might otherwise be unmanageably large. The requirements for volumes only apply to the aggregations at the activity level. They are intended to be primarily useful for physical files in hybrid systems.

Where the digital records management system uses volumes, it **shall**:

82	Allow administrators to add (open) digital volumes to any digital aggregation that is not closed.
83	Record the date of opening of a new volume in the volume's records management metadata.

12 That is, it shall be impossible for a situation to arise where any user action or any software failure results in an inconsistency within the digital records management system or its database.

13 Other criteria may be desirable in particular circumstances, for example, where the size of the volume reaches the capacity of storage media.

84	Automatically include in the metadata of new volumes those attributes of its parent aggregation's records management metadata that assign context (for example, name, classification code).
85	Support the concept of open and closed volumes for digital aggregations, as follows: 1. only the most recently created volume within an aggregation can be open; and 2. all other volumes within that aggregation shall be closed (subject to temporary exceptions required by Requirement 68).[14]
86	Prevent the user from adding digital records to a closed volume (subject to the exceptions required by Requirement 68).
87	Allow an administrator to add records to a closed file.[15]

14 Note that the records in a volume can be accessed regardless of whether the volume is open or closed.

15 This facility is intended to be used to rectify user error, for example, if a volume has been closed unintentionally.

5.4 MAINTAIN

5.4.1 Access and security

Organisations need to control access to their records and differing levels. Typically, access to records and aggregations is limited to specific users and/or user groups. In addition to controlling access by user and user groups, some organisations will need to limit access further by using security classifications. This is achieved by allocating security classifications to a user role, an aggregation of records or at an individual records level. Users can then be allocated security clearances to permit selective access to aggregations or records at higher security categories.

The digital records management system **shall**:

88	Ensure that records are maintained complete and unaltered, except in circumstances such as court orders for amendments to record content and metadata, in which cases only system administrators may undertake such changes with appropriate authorisation.
89	Document any exceptional changes to records as described in Requirement 88 in relevant metadata.
90	Maintain the technical, structural and relational integrity of records and metadata in the system.

5.4.2 Access controls

The digital records management system **shall**:

91	Restrict access to system functions according to a user's role and strict system administration controls.[16]

5.4.3 Establishing security control

Systematic security controls over access, discoverability and search support the maintenance of authenticity, reliability, integrity and usability, and therefore should be appropriately implemented.

A risk assessment can inform business decisions as to how rigorous the controls need to be. For example, in a high-risk environment, it may be necessary to prove exactly what happened, when and by whom at a very detailed or granular level. This links to systems permissions and audit logging, to prove that approved actions are undertaken by authorised people.

The digital records management system **shall**:

92	Allow only administrators to set up user profiles and allocate users to groups.
93	Allow the administrator to limit access to records, aggregations and records management metadata to specified users or user groups.

16 For example, an unauthorised user access attempt.

94	Allow the administrator to alter the security category of individual records.[17]
95	Allow changes to security attributes for groups or users (such as access rights, security level, privileges, initial password allocation and management) to be made only by the administrator.

5.4.4 Assigning security levels

The digital records management system **shall**:

96	Allow only the administrator to attach to the user profile attributes that determine the features, records management metadata fields, records or aggregations to which the user has access. The attributes of the profile will: 1. prohibit access to the digital records management system without an accepted authentication mechanism attributed to the user profile; 2. restrict user access to specific records or aggregations; 3. restrict user access according to the user's security clearance; 4. restrict user access to particular features (for example, read, update and/or delete specific records management metadata fields); 5. deny access after a specified date; and 6. allocate the user to a group or groups.[18]
97	Be able to provide the same control functions for roles, as for users.[19]
98	Be able to set up groups of users that are associated with an aggregation.[20]
99	Allow a user to be a member of more than one group.

If the digital records management system maintains a list of aggregations, it **shall**:

100	Be able to limit users' access to parts of the list (to be specified at the time of configuration).
101	Allow a user to stipulate which other users or groups can access records that the user is responsible for.[21]

5.4.5 Executing security controls

The digital records management system **shall**:

17 This is routinely required to reduce the level of protection given to records as their sensitivity decreases over time.

18 An example of an accepted authentication mechanism is a password.

19 This feature allows the administrator 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 Officer, Security Analyst or Database Administrator.

20 Examples of groups might be Personnel or Sales Team.

21 This function should be granted to the user by the administrator according to the organisation's policy.

102	Allow the administrator, subject to Section 5.4.6: Security categories, to alter the security category of all records within an aggregation in one operation. The digital records management system shall provide a warning if the security classifications of any records are lowered, and await confirmation before completing the operation.[22]
103	Allow the administrator to change the security category of aggregations, subject to the requirements of Section 5.4.6: Security categories.
104	Record full details of any change to security category in the records management metadata of the record, volume or aggregation affected.
105	Provide one of the following responses (selectable at configuration time) whenever a user requests access to, or searches for, a record, volume or aggregation that they do not have the right to access: 1. display title and records management metadata; 2. display the existence of an aggregation or record (that is, display its file or record number) but not its title or other records management metadata; or 3. not display any record information or indicate its existence in any way.[23]
106	Never include, in a list of full text or other search results, any record that the user does not have the right to access.[24]

If the digital records management system allows users to make unauthorised attempts to access aggregations (and their volumes) or records, it **shall**:

107	Log all unauthorised attempts to access aggregations (and their volumes) or records in their respective unique metadata.[25]

5.4.6 Security categories

The functional requirements in this section only apply to organisations that manage classified records within their digital records management system. Please refer to your local legislative requirements and security requirements.

The digital records management system **shall**:

108	Allow security classifications to be assigned to records.[26]

22 This is routinely required to reduce the level of protection given to records as their sensitivity decreases over time.

23 These options are presented in order of increasing security. NOTE that the requirement in the third option (that is, the most stringent) implies that the digital records management system shall not include such records in any count of search results.

24 Note that if the first option of Requirement 103 is chosen, Requirement 104 may appear to be in conflict with it. 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.

25 It will be acceptable for this feature to be controllable so that it only applies to administrator-specified security categories. Although the system should capture the location/interface and user or user log-in that attempted to gain access.

109	Allow security classifications to be selected and assigned at system level for: 1. all levels of records aggregations (including volumes); and 2. individual records or record objects.
110	Allow access-permission security categorisation to be assigned: 1. at group level (be able to set up group access to specific aggregations, record classes security or clearance levels); 2. by organisational role; 3. at user level; and 4. in combination(s) of the above.[27]
111	Allow the assignment of a security category: 1. at any level of records aggregation; 2. after a specified time or event; and 3. to a record type.[28]
112	Support the automated application of a default value of 'Unclassified' to an aggregation or record not allocated any other security category.
113	Enable its security subsystem to work effectively together with general security products.
114	Be able to determine the highest security category of any record in any aggregation by means of one simple enquiry.
115	Support routine, scheduled reviews of security classifications.
116	Restrict access to digital aggregations/records that have a security classification higher than a user's security clearance.

If security classifications are assigned to aggregations as well as individual records (as per Requirement 107), then the digital records management system **shall**:

---

26 Security classification will be jurisdictionally or organisationally assigned but may include category levels such as:

• Unclassified;

• In Confidence (policy and privacy);

• Sensitive (policy and privacy);

• Restricted (national security information);

• Confidential (national security information);

• Secret (national security information); and

• Top Secret (national security information).

Further caveats may be assigned to any security clearance levels.

27 This will allow an administrator to manage and maintain a limited set of access-permissions/categories based on roles within the organisation rather than managing a large number of individual user-permission profiles for classified access.

28 Note that the correct level of security clearance may not be sufficient to obtain access. Searches will block access by not returning search results for records that are above a searcher's access clearance, see Requirements 103 and 104.

117	Be capable of preventing a digital aggregation from having a lower security classification than any digital record within that aggregation.

5.4.7 Records management process metadata

Metadata about the processes of managing the record, including the disposition of the record, needs to be documented to ensure the integrity and authenticity of the record, so that all alterations, linkages and uses of the record are able to be authoritatively tracked over time. Records exist at different layers of aggregation, for example, as documents, items, files or series. Records management metadata shall be applied to records at all levels of aggregations. Although the record may be fixed and inviolable, the records management metadata will continue to accrue throughout the administrative life of the record. It shall be persistently linked to the record to ensure that the record is authentic, unaltered and reliable.

The digital records management system **shall**:

118	Be capable of creating unalterable metadata of records management actions (actions to be specified by each organisation) that are taken on records, aggregations or the classification scheme. The metadata should include the following records management metadata elements: 1. type of records management action; 2. user initiating and/or carrying out the action; and 3. date and time of the action.[29]
119	Track events, once the metadata functionality has been activated, without manual intervention, and store in the metadata information.
120	Maintain the metadata for as long as required.
121	Provide metadata of all changes made to: 1. digital aggregations (including volumes); 2. individual digital records; and 3. records management metadata associated with any of the above[30].
122	Document all changes made to administrative parameters (for example, changes made by the administrator to a user's access rights).

29 The word 'unalterable' means that the metadata data cannot be modified in any way or deleted by any user. It may be subject to re-organisation and copying to removable media if required by, for example, database software, so long as its content remains unchanged and for a specific purpose.

30 This process shall not alter the original metadata data.

123	Be capable of capturing and storing in the metadata information about the following actions: 1. date and time of capture of all digital records; 2. reclassification of a digital record in another digital volume; 3. reclassification of a digital aggregation in the classification scheme; 4. any change to the disposition authority of a digital aggregation; 5. any change made to any records management metadata associated with aggregations or digital records; 6. date and time of creation, amendment and deletion of records management metadata; 7. changes made to the access privileges affecting a digital aggregation, digital record or user; 8. export or transfer actions carried out on a digital aggregation; 9. date and time at which a record is rendered; and 10. disposition actions on a digital aggregation or record.
124	Ensure that metadata is available for inspection on request, so that a specific event can be identified and all related data made accessible, and that this can be achieved by authorised external personnel who have little or no familiarity with the system.
125	Be able to export metadata for specified records and selected groups of records without affecting the metadata stored by the digital records management system.[31]
126	Be able to capture and store violations (that is, a user's attempts to access a record or aggregation, including volumes, to which they are denied access), and (where violations can validly be attempted) attempted violations of access control mechanisms.[32]
127	Be able, at a minimum, to provide reports for actions on records and aggregations organised: 1. by record or aggregation; 2. by user; and 3. in chronological sequence.
128	Allow the metadata facility to be configurable by the administrator so that the functions for which information is automatically stored can be selected. The digital records management system shall ensure that this selection and all changes to it are stored in the metadata.

31 This functionality can be used by external auditors who wish to examine or analyse system activity.

32 It is acceptable for this feature to be controllable so that it only applies to administrator-specified security categories.

129	Be able to provide reports for actions on aggregations and records organised by workstation and (where technically appropriate) by network address.
130	Allow the administrator to change any user-entered records management metadata element. Information about any such change shall be stored in the metadata.[33]

5.4.8 Tracking record movement

Location can refer to the physical location of a hybrid record or the location within a classification structure or file structure for digital records. Movement refers to changing the location of both digital and physical records.

The digital records management system **shall**:

131	Provide a tracking feature to monitor and record information about the location and movement of both digital and non-digital aggregations.
132	Record information about movements including: 1. unique identifier of the aggregation or record; 2. current location as well as a user-defined number of previous locations (locations should be user-defined); 3. date item sent/moved from location; 4. date item received at location (for transfers); and 5. user responsible for the move (where appropriate).
133	Maintain access to the digital record content, including the ability to render it, and maintenance of its structure and formatting over time and through generations of office application software.[34]

33 This functionality is intended to allow administrators to correct user errors, such as data input errors, and to maintain user and group access.

34 This may be achieved by use of a multi-format viewer application.

5.5 Hybrid records management

5.5.1 Management of digital and non-digital records

Not all digital records management systems are limited to the management of records in digital format; some are specifically designed to provide for the management of physical records as well. Consequently, the functional requirements include requirements for hybrid system management to include functionality for managing records and files in both digital and physical format.

5.5.1.1 Hybrid file

The relationship between physical files and records in digital formats differs significantly. As physical objects, non-digital records (such as paper-based files) cannot be physically captured and registered directly into the business system. They require a digital component to bind them to other digital objects. A digital records management system shall create and maintain markers (metadata profiles of physical or digital records) to create and maintain the linkages between the physical and digital files.

Generally the marker will identify the title and unique identifier of the physical record, outline the record's content and provide location information for retrieval.

A hybrid file exists where a related set of physical files and aggregations of digital records (for example, digital files) deals with the same function, activity or transaction, and shall be managed as a single aggregation of records. Management of these hybrid files involves merging the aggregation of digital records and physical file management processes.

5.5.1.2 Hybrid records

Digital records can be linked to physical records or files through a tightly bound metadata relationship to form a hybrid record or hybrid file in much the same way that physical files and aggregations of digital records can be linked to create hybrid files. The metadata link between the digital and physical records is established through the marker, which identifies the physical record and its location. The marker may be attached directly to the digital record component of the hybrid record or be created and related separately.

The digital records management system **shall**:

134	Be able to define in the classification scheme non-digital aggregations and volumes, and shall allow the presence of non-digital records in these volumes to be reflected and managed in the same way as digital records.
135	Allow both kinds of record to be managed in an integrated manner.
136	Allow a non-digital aggregation that is associated as a hybrid with a digital aggregation to use the same title and numerical reference code, but with an added indication that it is a hybrid non-digital aggregation.

137	Allow a different records management metadata element set to be configured for non-digital and digital aggregations; non-digital aggregation records management metadata shall include information on the physical location of the non-digital aggregation.
138	Ensure that retrieval of non-digital aggregations displays the records management metadata for both digital and non-digital records associated with it.
139	Include features to control and record access to non-digital aggregations, including controls based on security category, which are comparable with the features for digital aggregations.
140	Support tracking of non-digital aggregations by the provision of request, check-out and check-in facilities that reflect the current location of the item concerned.

The digital records management system **should**:

141	Support the printing and recognition of bar codes for non-digital objects (for example, documents, files and other containers), or should support other tracking systems to automate the data entry for tracking the movement of such non-digital records.
142	Support the retention and disposition protocols and routinely apply to both digital and non-digital elements within hybrid aggregations.

Where aggregations have security categories, the digital records management system **shall**:

143	Ensure that a non-digital record is allocated the same security category as an associated digital record within a hybrid records aggregation.

5.6 Retention and disposition

5.6.1 Disposition authorities

Records usually cannot be disposed of without a valid and authorized retention and disposition authority. They set a minimum period of time before a disposition action can be applied to a record. 'Destroy' or 'Retain as permanent archive' are the most common disposition actions for records. Records destruction is a straightforward process of destroying the physical manifestation of a non-digital record; it is a more complex undertaking for digital records.

Deletion is often considered to be (permanent) destruction; however material may still be accessible, discoverable or recoverable due to back-ups, personal hard drives and so on, and through digital forensics. These technical issues may be addressed at a policy or technical level and may require serious consideration where legislative or security requirements are paramount.

5.6.1.1 Establishing disposition authorities

The digital records management system **shall**:

144	Provide a function that: 1. specifies disposition authorities; 2. automates reporting and destruction actions; 3. disposes of compound records as a single action; and 4. provides integrated facilities for exporting records and records management metadata.
145	Be able to restrict the setting up and changing of disposition authorities to the administrator only.
146	Allow the administrator to define and store a set of customised standard disposition authorities.
147	Support retention periods from a minimum of one month to an indefinite period.

5.6.1.2 Applying disposition authorities

The digital records management system **shall**:

148	Be capable of assigning a disposition authority to any aggregation or record type.
149	By default, ensure that every record in an aggregation is governed by the disposition authority(s) associated with that aggregation.
150	Include a disposition action, organisation retention period and trigger in the (metadata) record for the decision for each disposition authority.
151	For each aggregation: 1. automatically track retention periods that have been allocated to the aggregation; and 2. initiate the disposition process by prompting the administrator to consider and, where appropriate approve and execute, disposition action when disposition is due.

152	Allow at least the following decisions for each disposition authority: 1. retain indefinitely; 2. present for review at a future date; 3. destroy at a future date; and 4. transfer at a future date.
153	Allow retention periods for each disposition authority to be specified at a future date, with the date able to be set in at least the following ways: 1. passage of a given period of time after the aggregation is opened; 2. passage of a given period of time after the aggregation is closed; 3. passage of a given period of time since the most recent record has been assigned to the aggregation; 4. passage of a given period of time after a specific event (event to be identified in the schedule, and will be notified to the digital records management system by the administrator, rather than being detected automatically by the digital records management system); and 5. specified as 'indefinite' to indicate long-term preservation of the records.[35]
154	Enable a disposition authority to be assigned to an aggregation that over-rides the disposition authority assigned to its 'parent' aggregation.[36]
155	Allow the administrator to amend any disposition authority allocated to any aggregation at any point in the life of that aggregation.
156	Allow the administrator to change the authority(s) associated with an aggregation at any time.
157	Allow the definition of sets of processing rules that can be applied as an alerting facility to specified aggregations prior to initiation of a disposition process.[37]
158	Provide the option of allowing digital records or aggregations that are being moved between aggregations by the administrator to have the disposition authority of the new aggregation, replacing the existing disposition authority(s) applying to these records.

5.6.1.3 Executing disposition authorities

The digital records management system **shall**:

159	Allow the administrator to delete aggregations, volumes and records (subject to Section 5.4.6: Security categories).[38]

35 While these are generally inclusive, it is possible that some records will have types of retention requirements that are not listed.

36 For example, if an aggregation ('parent') contains another aggregation ('child'), then it shall be possible to assign a disposition authority to the 'child' that over-rides the disposition authority for the 'parent'.

37 For example, during a review of the aggregation and contents by a manager or administrator, notify the administrator when an aggregation has a given security level.

38 This functionality is intended for exceptional circumstances only.

160	When executing disposition authorities, the digital records management system shall be able to: 1. produce an exception report for the administrator; 2. delete the entire contents of an aggregation or volume when it is deleted; 3. prompt the administrator to enter a reason for the action; 4. ensure that no items 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 Section 3.1.3: Aggregation of digital records – one of which is being deleted); 5. inform the administrator of any links from another aggregation or record to an aggregation or volume, that is about to be deleted, and request confirmation before completing the deletion; 6. alert the administrators to any conflicts, for example, items that are linked to more than one disposition action involving pointers; and 7. maintain complete integrity of the records management metadata at all times.

If more than one disposition authority is associated with an aggregation, the digital records management system **shall**:

161	Automatically track all retention periods specified in these disposition authorities, and initiate the disposition process once the last of all these retention dates is reached.
162	Allow the administrator to manually or automatically lock or freeze records disposition processes (e.g. a freeze for litigation or legal discovery purposes, Freedom of Information purposes, and so on.).

5.6.1.4 Documenting disposition actions

The digital records management system **shall**:

163	Record any deletion or disposition action comprehensively in the process metadata.
164	Automatically record and report all disposition actions to the administrator.

5.6.1.5 Reviewing disposition

The digital records management system **shall**:

165	Support the review process by presenting digital aggregations to be reviewed, with their records management metadata and disposition authority information, in a manner that allows the reviewer to browse the contents of the aggregation and/or records management metadata efficiently.

166	Allow the reviewer to take at least any one of the following actions for each aggregation during review: 1. mark the aggregation for destruction; 2. mark the aggregation for transfer; 3. mark the aggregation for indefinite hold, for example, pending litigation; and 4. change the disposition authority (or assign a different schedule) so that the aggregation is retained and re-reviewed at a later date, as defined in this section.
167	Allow the reviewer to enter comments into the aggregation's records management metadata to record the reasons for the review decisions.
168	Alert the administrator to aggregations due for disposition before implementing disposition actions, and on confirmation from the administrator shall be capable of initiating the disposition actions specified in this section.
169	Store in the metadata all decisions taken by the reviewer during reviews.
170	Produce a disposition authority report for the administrator that identifies all disposition authorities that are due to be applied in a specified time period, and provide quantitative reports on the quantity and types of records covered.
171	Be able to specify the frequency of a disposition authority report, the information reported and highlight exceptions such as overdue disposition.
172	Alert the administrator if a digital aggregation that is due for destruction is referred to in a link from another aggregation and pause the destruction process to allow the following remedial action to be taken: 1. confirmation by the administrator to proceed with or cancel the process; and 2. generation of a report detailing the aggregation or record(s) concerned and all references or links for which it is a destination.
173	Support reporting and analysis tools for the management of retention and disposition authorities by the administrator, including the ability to: 1. list all disposition authorities; 2. list all digital aggregations to which a specified disposition authority is assigned; 3. list the disposition authority(s) applied to all aggregations below a specified point in the hierarchy of the classification scheme; 4. identify, compare and review disposition authorities (including their contents) across the classification scheme; and 5. identify formal contradictions in disposition authorities across the classification scheme.
174	Provide, or support the ability to interface with, a workflow facility to support the scheduling, review and export/transfer process by tracking: 1. progress/status of the review, such as awaiting or in-progress, details of reviewer and date; 2. records awaiting disposition as a result of a review decision; and 3. progress of the transfer process.

The digital records management system **should**:

175	Be able to accumulate statistics of review decisions in a given period and provide tabular and graphic reports on the activity.

5.6.2 Migration, export and destruction

The digital records management system **shall**:

176	Provide a well-managed process to transfer records to another system or to a third party organisation and support migration processes.
177	Include all aggregations, volumes, records and associated metadata within aggregations whenever a digital records management system transfers any aggregation or volume.
178	Be able to transfer or export an aggregation (at any level) in one sequence of operations so that: 1. the content and structure of its digital records are not degraded; 2. all components of a digital record (when the record consists of more than one component) are exported as an integral unit including any technical protection measures; 3. all links between the record and its records management metadata are retained; and 4. all links between digital records, volumes and aggregations are retained.
179	Be able to include a copy of the entire metadata set associated with the records and aggregations that are transferred or exported from a digital records management system.
180	Produce a report detailing any failure during a transfer, export or destruction. The report shall identify any records destined for transfer that have generated processing errors and any aggregations or records that are not successfully transferred, exported or destroyed.
181	Retain copies of all digital aggregations and their records that have been transferred, at least until such time as a successful transfer is confirmed.[39]
182	Be able to continue to manage records and aggregations that have been exported from the digital records management system to other forms of storage media.
183	Have the ability to retain records management metadata for records and aggregations that have been destroyed or transferred.
184	Allow the administrator to specify a subset of aggregation records management metadata that will be retained for aggregations which are destroyed, transferred out or moved offline.[40]

39 This is a procedural safeguard to ensure that records are not deleted before successful transfer is confirmed.

40 This is necessary for the organisation to know which records it has held and the dates they were destroyed or disposed of, without necessarily incurring the expense of keeping all the detailed records management metadata for the records.

185	Enable the total destruction of records (whether identified by class or individually) stored on re-writable media by completely obliterating them so that they cannot be restored through specialist data recovery facilities.

The digital records management system **should**:

186	Provide a utility or conversion tool to support the conversion of records marked for transfer or export into a specified file transfer or export format.
187	Provide the ability to add user-defined records management metadata elements required for archival management purposes to digital aggregations selected for transfer.
188	Provide the ability to sort digital aggregations selected for transfer into ordered lists according to user-selected records management metadata elements.

Where hybrid aggregations are to be transferred, exported or destroyed, the digital records management system **shall**:

189	Require the administrator to confirm that the non-digital part of the same aggregations has been transferred, exported or destroyed before transferring, exporting or destroying the digital part.

5.6.3 Retention and disposition of digital and non-digital records

The digital records management system **shall**:

190	Support the allocation of disposition authorities to every non-digital aggregation in the classification scheme. The authorities shall function consistently for digital and non-digital aggregations, notifying the administrator when the disposition date is reached, but taking account of the different processes for disposing of digital and non-digital records.
191	Support the application of the same disposition authority to both the digital and non-digital aggregations that make up a hybrid aggregation.
192	Be able to apply any review decision made on a hybrid digital aggregation to a non-digital aggregation with which it is associated.
193	Alert the administrator to the existence and location of any hybrid non-digital aggregation associated with a hybrid digital aggregation that is to be exported or transferred.
194	Be able to record in the metadata all changes made to records management metadata references to non-digital or hybrid aggregations and records.
195	Be capable of offering check-out and check-in facilities for non-digital aggregations profiled in the system, in particular enabling the ability to record a specific user or location to which a non-digital aggregation is checked out, and to display this information if the non-digital aggregation is requested by another user.
196	Be capable of offering a request facility for non-digital records profiled in the hybrid aggregation system, enabling a user to enter a date that the non-digital element is required and generating a consequent message for transmission to the current holder of that non-digital aggregation or the administrator, according to configuration.
197	Be able to export and transfer records management metadata of non-digital records and aggregations.

The digital records management system **should**:

198	Support the application of a review decision taken on a group of aggregations to any non-digital aggregations within that group, by notifying the administrator of necessary actions to be taken on the non-digital aggregations.

5.7 DISSEMINATE

5.7.1 Search, retrieve and render

A digital records management system has to be able to reproduce content that is intended to be human-readable on demand in a way that it is timely and not technically problematic or onerous. It is also essential that digital records management systems never present information to any user who is not authorised to access it. All the features and functionality in this section shall be subject to access controls as described in *Section 5.4.1: Access and security*. To avoid complexity, this is assumed and is not repeated in each requirement below.

The digital records management system **shall**:

199	Provide a flexible range of functions that operate on the metadata related to every level of aggregation and on the contents of the records through user-defined parameters for the purpose of locating, accessing and retrieving individual records or groups of records and/or metadata.
200	Allow all record, volume and aggregation records management metadata to be searchable.
201	Allow the text contents of records (where they exist) to be searchable.
202	Allow the user to set up a single search request with combinations of records management metadata and/or record content.
203	Allow administrators to configure and change the search fields to: 1. specify any element of record, volume and aggregation records management metadata, and optionally full record content, as search fields; and 2. change the search field configuration.
204	Provide searching tools for: 1. free-text searching of combinations of record and aggregation records management metadata elements and record content; and 2. Boolean searching of records management metadata elements (see also Requirement 219).
205	Provide for 'wild card' searching of records management metadata that allows for forward, backward and embedded expansion.[41]
206	Allow searching within a single aggregation or across more than one aggregation.
207	Be able to search for, retrieve and display all the records and records management metadata relating to a digital aggregation, or volume, as a single unit.
208	Be able to search for, retrieve and render a digital aggregation by all implemented naming principles, including: 1. name; and 2. identifier (classification code).

41 For example, the search term 'proj*' might retrieve 'project' or 'PROJA'; the term 'C*t' would retrieve 'Consultant'.

209	Display the total number of search results on a user's screen and shall allow the user to then display the results list, or refine the search criteria and issue another request.
210	Allow records and aggregations featured in the search results list to be selected, then opened (subject to access controls) by a single click or keystroke.
211	Allow users to retrieve aggregations and records directly through the use of a unique identifier.
212	Never allow a search or retrieval function to reveal to a user any information (records management metadata or record content) that the access and security settings are intended to hide from that user.
213	Have integrated search facilities for all levels of the classification scheme.[42]
214	Provide free-text and records management metadata searches in an integrated and consistent manner.
215	Present seamless functionality when searching across digital, non-digital and hybrid aggregations.
216	Allow users to save and re-use queries.
217	Allow users who are viewing or working with a record or aggregation, whether as the result of a search or otherwise, to see the record within the classification or aggregation hierarchy easily and without leaving or closing the record.[43]
218	Allow users to refine (that is, narrow) searches.[44]

The digital records management system **should**:

219	Provide word proximity searching that can specify that a word has to appear within a given distance of another word in the record to qualify as a search result (see also Requirements 202, 203 and 204).
220	Allow the records management metadata of any object (such as record, volume or aggregation) to be searched, whether the object itself is in digital form or not, and regardless of whether the object is stored online, near-line or offline.

42 In other words, users should see the same interface, features and options whether searching for classes, aggregations or records.

43 For example, when reading a record, the user should be able to see what volume and aggregation the record is associated with. If viewing aggregation records management metadata, the user should be able to find out information about the aggregation in which it is located.

44 For example, a user should be able to start with the result list from a search and then initiate a further search within that list.

221	Provide display formats configurable by users or administrators for search results, including such features and functions as: 1. select the order in which the search results are presented; 2. specify the number of search results displayed on the screen; 3. set the maximum number of search results; 4. save the search results; and 5. choose which records management metadata fields are displayed in search result lists.
222	Provide relevance ranking of the search results.
223	Be able to relate an 'extract' of a digital record to the original record, so that retrieval of one allows retrieval of the other, while retaining separate records management metadata and access controls over the two items.
224	Provide concept searches through the use of a thesaurus incorporated as an online index.[45]

Where a graphical user interface is employed, the digital records management system **shall**:

225	Provide a browsing mechanism that enables graphical or other display browsing techniques at any level of aggregation.[46]

5.7.2 Rendering: displaying records

The digital records management system **shall**:

226	Render or download records that the search request has retrieved.[47]

The digital records management system **should**:

227	Render records that the search request has retrieved without loading the associated application software.[48]
228	Be able to render all the types of digital records specified by the organisation in a manner that preserves the information in the records (for example, all the features of visual presentation and layout produced by the generating application package), and which renders all components of a digital record in their original relationship.[49]

[45] This will allow retrieval of documents with a broader, narrower or related term in their content or records management metadata. For example, a search for 'ophthalmic services' might retrieve 'health services', 'eye test' or 'ophthalmology'.

[46] This would be used with the searching techniques described above to provide a first-level view of records management metadata for a group of records or aggregations that have met the specified search criteria.

[47] If the digital records management system is storing records in a proprietary application format, it may be acceptable for the rendering to be performed by an application outside the digital records management system.

[48] This is typically provided by integrating a viewer software package into the digital records management system. This is frequently desirable to increase speed of rendering.

[49] The organisation shall specify the application packages and formats required.

5.7.3 Rendering: printing

This section applies to records and their records management metadata and other data within the digital records management system that can meaningfully be printed.

The digital records management system **shall**:

229	Provide the user with flexible options for printing records and their relevant records management metadata, including the ability to print a record(s) with records management metadata specified by the user.
230	Allow the printing of records management metadata for an aggregation.
231	Allow the user to be able to print out a summary list of selected records (for example, the contents of an aggregation), consisting of a user-specified subset of records management metadata elements (for example, Title, Author, Creation date) for each record.
232	Allow the user to print the results list from all searches.
233	Be able to print all the types of digital records specified by the organisation. Printing shall preserve the layout produced by the generating application package(s) and include all (printable) components of the digital record.[50]
234	Allow the administrator to specify that all printouts of records have selected records management metadata elements appended to them, for example, title, registration number, date and security category.
235	Allow the administrator to print the thesaurus, where a thesaurus exists within the system.
236	Allow the administrator to print any and all administrative parameters.
237	Allow the administrator to print disposition authorities.
238	Allow the administrator to print the classification scheme.
239	Allow the administrator to print metadata schema or element sets.

The digital records management system **should**:

240	Allow all records in an aggregation to be printed, in the sequence specified by the user, in one operation.

If the digital records management system uses classification schemes and thesauri, it **shall**:

241	Allow the administrator to print the file list.

5.7.4 Rendering: redacting records

A redacted record is a copy of a digital record from which some material has been removed or permanently masked (redacted). An extract is made when the full record cannot be released for access, but part of the record may be..

The digital records management system **shall**:

[50] The organisation shall specify the application packages and formats required.

242	Allow the administrator to take a copy of a record for the purposes of redaction.[51]
243	Record the creation of extracts in the records management metadata, including at least date, time, reason for creation and creator.
244	Store in the metadata any change made in response to the requirements in this section.

The digital records management system **should**:

245	Provide functionality for redacting (see Glossary at Appendix A) sensitive information from the extract. If the digital records management system does not directly provide these facilities, it shall allow for other software packages to do so.[52]
246	Prompt the creator of an extract to assign it to an aggregation.
247	Store a cross-reference to an extract in the same aggregation and volume as the original record, even if that volume is closed.

5.7.5 Rendering: other

This section applies only to records that cannot meaningfully be printed, such as audio, visual and database files.

The digital records management system **shall**:

248	Include features for rendering those records that cannot be meaningfully printed to an appropriate output device.[53]

[51] This copy is referred to as an 'extract' of the record in this requirement.

[52] It is essential that when these or any other redaction features are used, none of the removed or masked information can ever be seen in the extract, whether on screen, printed or played back, regardless of the use of any features such as rotation, zooming or any other manipulation.

[53] Examples include audio, video and some websites.

5.8 ADMINISTER

5.8.1 Administration

In exceptional circumstances, record content may be altered or deleted by system administrators. Where this is the case, the system shall be able to create redacted copies of records. System administrators also need to be able to manage system parameters, back up and restore data, and generate system reports. This section includes requirements for managing system parameters, back-up and restoration, system management and user administration. The administration of security classification and controls are addressed in the relevant security-related requirements in *Section 5.4.1: Access and security*.

5.8.2 Administrator functions

The digital records management system **shall**:

250	Allow the administrator to retrieve, display and re-configure system parameters and to re-allocate users and functions between user roles.
251	Provide back-up facilities so that records and their records management metadata can be recreated using a combination of restored back-ups and metadata.
252	Provide recovery and rollback[54] facilities in the case of system failure or update error, and shall notify the administrator of the results.[55]
253	Monitor available storage space and notify the administrator when action is needed because available space is at a low level or because it needs other administrative attention.
254	Allow the administrator to make bulk changes to the classification scheme, ensuring all records management metadata and metadata data are handled correctly and completely at all times, in order to make the following kinds of organisational change: 1. division of an organisational unit into two; 2. combination of two organisational units into one; 3. movement or re-naming of an organisational unit; and 4. division of a whole organisation into two organisations.[56]

[54] A rollback is the undoing of partly completed changes when a transaction is determined to have failed.

[55] That is, the digital records management system shall allow administrators to 'undo' a series of transactions until a status of assured database integrity is reached. This is only required when error conditions arise.

[56] When such a change is made, closed files shall remain closed, retaining their references to the classification scheme before the change, and open files shall either be closed, retaining their references to the classification scheme before the change and cross-referenced to a new file in the changed scheme, or be referenced to the changed scheme, but clearly retaining all prior references to the classification scheme before the change. Changes to organisational units described above may imply corresponding changes to the classification schemes of the units and their user populations. The term 'bulk changes' implies that all aggregations and records affected can be processed with a small number of transactions, rather than needing to be processed individually.

255	Support the movement of users between organisational units.
256	Allow the definition of user roles, and shall allow several users to be associated with each role.
257	Communicate any errors encountered in saving data to storage media.

5.8.3 Metadata administration

Metadata schemas shall be administered, including the creation, addition, deletion or alteration of metadata elements, and any semantic and syntactical rules and obligation status applied to those elements.

The digital records management system **shall**:

258	Allow the administrator to create, define and delete metadata elements, including custom fields.
259	Allow the administrator to apply and modify metadata schema rules, including semantic and syntactical rules, encoding schemes and obligation status.
260	Allow the administrator to configure the system to restrict the viewing or modifying of metadata elements by group, functional role or user.
261	Document all metadata administration activities.

5.8.4 Reporting

This section articulates basic reporting requirements. It does not articulate the requirements for a comprehensive reporting subsystem.

The digital records management system **shall**:

262	Provide flexible reporting facilities for the administrator. They shall include, at a minimum, the ability to report the following: 1. numbers of aggregations, volumes and records; 2. transaction statistics for aggregations, volumes and records; and 3. activity reports for individual users.
263	Allow the administrator to report on metadata based on selected: 1. aggregations; 2. volumes; 3. record objects; 4. users; 5. time periods; and 6. file formats and instances of each format.
264	Be able to produce a report listing aggregations, structured to reflect the classification scheme, for all or part of the classification scheme.
265	Allow the administrator to request regular periodic reports and one-off reports.

Note that this element will apply especially where classification schemes are based on an organisation plan and be less necessary where classification is functionally assessed.

266	Allow the administrator to report on metadata based on selected: 1. security categories; 2. user groups; and 3. other records management metadata.
267	Include features for sorting and selecting report information.
268	Include features for totalling and summarising report information.
269	Allow the administrator to restrict users' access to selected reports.

5.8.5 Back-up and recovery

Digital records management systems shall have comprehensive controls to create regular back-ups of the records and records management metadata that they maintain. These back-ups should enable the digital records management system to rapidly recover records if any are lost because of system failure, accident or security breach. In practice, back-up and recovery functions may be divided between digital records management system administrators and IT staff. The process of "mirroring" servers is another way to capture records in real time and mitigate risks.

The digital records management system **shall**:

270	Provide automated back-up and recovery procedures.
271	Allow the administrator to schedule back-up routines by: 1. specifying the frequency of back-up; and 2. allocating storage media, system or location for the back-up (for example, offline storage, separate system, remote site).
272	Allow only the administrator to restore from digital records management system back-ups. Full integrity of the data shall be maintained after restoration.
273	Allow only the administrator to roll-forward the digital records management system from a back-up to a more recent state, maintaining full integrity of the data.
274	Allow users to indicate that selected records are considered to be 'vital records'.[57]
275	Be able to notify users whose updates may have been incompletely recovered, when they next use the system, that a potentially incomplete recovery has been executed.

[57] Vital records are those records that are absolutely necessary for the organisation's ability to continue its business either in terms of its ability to cope with emergency/disaster conditions or to protect its financial and legal interests. The identification and protection of such records, therefore, is of great importance to any organisation.

6. APPENDICES

Appendix A - Sample checklist of requirements for reviewing an existing digital records management system

This appendix gives guidance only. This tool provides a set of requirements for organisations to assess and existing digital records management system.

Table A.1 – Sample checklist of requirements

NOTE 1 This tool assumes that the digital records management system in question contains records and that the fundamental records management tools such as the disposition authority, business classification scheme, and security and access classification scheme are in place within the organisation.

No.	Checkpoint	Evidence of achievement / comments	Level of achievement (1–5): 5 = Satisfied 3 = Partially satisfied 1 = Not satisfied
GENERAL			
	Are personnel appropriately trained to be able to implement their records management responsibilities?		
CREATE RECORDS THAT ARE LINKED TO THEIR CONTEXT			
	Can ‘fixed’/static records be created by the system?		
	Can the system create records that are linked to their business context?		
	Does the system capture the required records management metadata elements in line with jurisdictional standards and business needs?		
	Is the records management metadata linked to the records, and are these linkages maintained over time?		

MANAGE AND MAINTAIN RECORDS			
	Are documented policies and procedures in place for the management of the records?		
	Can the records be proven to be what they purport to be; have been created or sent by the person that created or sent it; and have been created or sent at the time purported?		
	Are there sufficient controls to protect the records from unauthorised access, alteration, deletion and use?		
	Can the records be searched for, displayed and accessed in a meaningful way?		
	Are there policies and procedures in place for conducting records management audits on the system on a regular basis?		
	Are back-up and disaster recovery plans in place for the system?		
	Is a complete and current set of system documentation maintained (for example, specifications, manuals, design, integration, etc.)?		
	If digital signatures are in use, can the records be read as and when required?		
IMPORT AND EXPORT OF RECORDS AND INTEROPERABILITY			
	Where records are stored with one organisation, but the responsibility for management and control resides with another, are the responsibilities clearly understood, traceable and documented?		
	Are there processes and mechanisms in place which support ongoing access to records, in line with retention requirements, beyond the life of the system?		
	Are records capable of being transferred from the system to an archival institution for archiving?		
RETENTION AND DISPOSITION			
	Can you execute disposition actions in line with the disposition authority?		
	Are records being retained in line with disposition authorities, and not being deleted or overwritten?		
HYBRID SYSTEMS			
	Where the system manages both physical and digital records, does it support hybrid records management functionality?		

Appendix B - Bibliography

[1] ISO 15489-1:2001, *Information and documentation — Records management — Part 1: General.*

[2] ISO/TR 15489-1:2001, *Information and documentation — Records management — Part 2: Guidelines*

[3] ISO/TR 15801:2009, *Electronic management — Information stored electronically — Part 2: Recommendations for trustworthiness and reliability.*

[4] ISO16175-1, *Information and documentation - Principles and functional requirements for records in electronic office environments - Part 1: Overview and statement of principles*.

[5] ISO16175-3, *Information and documentation - Principles and functional requirements for records in electronic office environments – Part 3: Guidelines and functional requirements for records in business systems*.

[6] ISO 23081-1: 2006, *Information and documentation — Records management processes — Metadata for records — Part 1: Principles.*

[7] ISO 23081-2:2009, *Information and documentation — Managing metadata for records — Part 2: Conceptual and implementation issues.*

[8] ISO 2788:1986, *Documentation —* Guidelines *for the establishment and development of monolingual thesauri.*

[9] ISO 5964:1985, *Documentation — Guidelines for the establishment and development of multilingual thesauri.*

[10] International Council on Archives, *Principles and Functional requirements for records in Electronic Office Environments, Part 1 — Overview and Statement of Principles*, 2008.

[11] International Council on Archives, *Principles and Functional requirements for records in Electronic Office Environments, Part 3 — Guidelines and Functional Requirements for Records in Business information systems*, 2008.

[12] Cornwell Management Consultants (for the European Commission Interchange of Documentation between Administrations Programme), Model Requirements for the Management of Digital Records, March 2001, http://www.cornwell.co.uk/moreq.

[13] International Council on Archives, Authenticity of Digital Records, ICA Study 13-1, November 2002.

[14] International Council on Archives, Authenticity of Digital Records, ICA Study 13-2, January 2004.

ICS 01.140.20

Price based on 61 pages