CONTINUUM

create & maintain

tāhuhu te hanga me te tiaki

ELECTRONIC RECORDKEEPING SYSTEMS STANDARD

ISSUED UNDER PUBLIC RECORDS ACT 2005. SECTION 27

SCOPE: ALL PUBLIC OFFICES AND LOCAL AUTHORITIES

STATUS: DISCRETIONARY BEST PRACTICE STANDARD

ARCHIVES NEW ZEALAND
TE RUA MAHARA O TE KĀWANATANGA
June 2005

Archives New Zealand
Te Whare Tohu Tuhituhinga O Aotearoa

RECORDKEEPING STANDARDS

S|5

CONTINUUM

create & maintain

tāhuhu te hanga me te tiaki

CONTINUUM
create & maintain
tāhuhu te hanga me te tiaki

ELECTRONIC RECORDKEEPING SYSTEMS STANDARD

ARCHIVES NEW ZEALAND

GOVERNMENT RECORDKEEPING GROUP

ISSUED UNDER PUBLIC RECORDS ACT 2005, SECTION 27
SCOPE: ALL PUBLIC OFFICES AND LOCAL AUTHORITIES
STATUS: DISCRETIONARY BEST PRACTICE STANDARD

S-5 STANDARD FOR FUNCTIONAL SPECIFICATIONS FOR ELECTRONIC RECORDKEEPING SYSTEMS

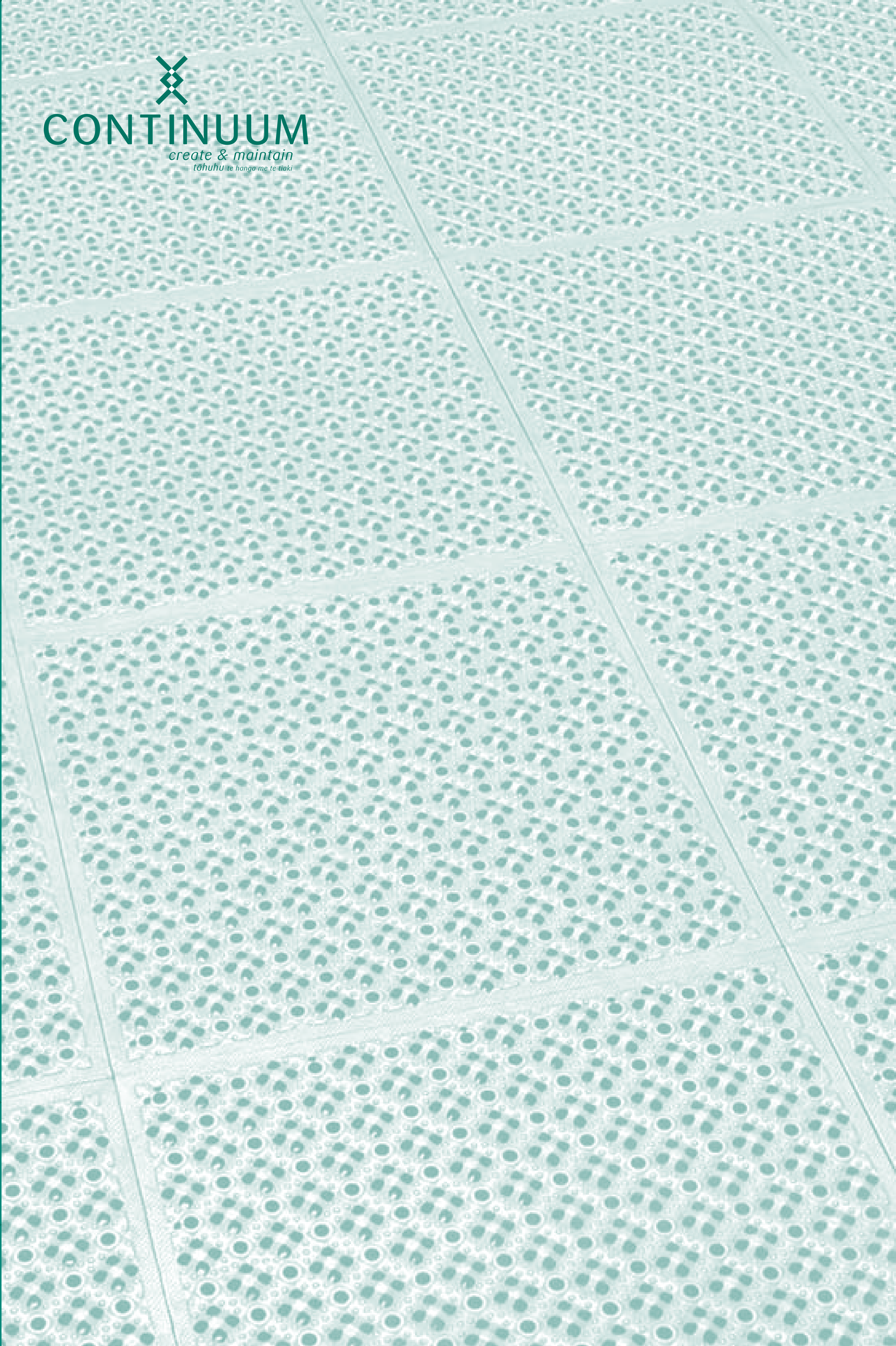
THIS STANDARD SETS OUT GUIDELINES AND FUNCTIONAL SPECIFICATIONS FOR ELECTRONIC RECORDKEEPING SYSTEMS USED BY PUBLIC OFFICES AND LOCAL AUTHORITIES.

CHIEF EXECUTIVE AND CHIEF ARCHIVIST

SIGNED: D. M. Macaskill

DATE: 29 June 2005

ELECTRONIC RECORDKEEPING SYSTEMS STANDARD
CONTINUUM CREATE & MAINTAIN
TĀHUHU TE HANGA ME TE TIAKI
ARCHIVES NEW ZEALAND
TE RUA MAHARA O TE KĀWANATANGA
June 2005



CONTINUUM

create & maintain

tāhuhu te hanga me te tiaki

ACKNOWLEDGEMENTS

This Standard was developed by Adam Stapleton, Archives Analyst, Archives New Zealand, with advice and guidance from a working party comprising:

- Sara Barham, Portal Information Manager, E-government Unit;
- Janine Delaney, Head Archivist, Context Control Unit, Archives New Zealand;
- Aaron Evans, Director, Zeta Consulting;
- Joanne Franks, Information Management Advisor, Ministry of Transport;
- Jackie Hill, Manager, Information Bureau, Ministry of Agriculture and Forestry;
- Tony Morine, Manager, Information Services, Department of Internal Affairs;

together with input from staff of the Government Recordkeeping Group of Archives New Zealand, including Alison Midwinter, Philippa Tucker, Mary Neazor and Sophie Young.

The Chief Archivist acknowledges the advice and guidance of the working party members, which has been central to the development of this Standard.

The specifications in this Standard draw on international professional literature and various institutional standards and policies. In particular, the Standard has adopted the distinction made by the electronic records and archives authority, David Bearman, between business information systems and recordkeeping systems. The specifications have drawn heavily upon the European Commission's *Model Requirements for the Management of Electronic Records: 'MoREQ' specification.*

CONTENTS

PART A > GENERAL

1 > INTRODUCTION

Good recordkeeping by government agencies is fundamental to a well-functioning democracy since it provides the mechanism whereby the public sector can account for its decisions and actions to Government and its citizens. Records also provide evidence for citizens to confirm or claim their rights and entitlements, as well as providing individual public servants with evidence to justify their decisions. Moreover, good recordkeeping is simply good business practice.

Recordkeeping systems facilitate:

- efficiency, by making information readily available when needed for decision-making and operational activities;
- sound use of financial resources, by allowing timely disposal of non-current records;
- accountability, by enabling the creation of a complete and authoritative record of official activities;
- compliance, by demonstrating that legal requirements have been met; and
- risk mitigation, by managing the risks associated with illegal loss or destruction of records, and from inappropriate or unauthorised access to records.

1.1 > PURPOSE

This Standard articulates a set of functional specifications for electronic recordkeeping systems for use within the New Zealand public sector. These specifications apply to records irrespective of the media in which they were created and stored. They are intended to:

- inform the selection of commercial 'off-the-shelf' electronic recordkeeping systems; and
- allow specifications for electronic recordkeeping systems to be incorporated into Request For Proposal documents (RFPs) during the initial stages of the development of new, or upgrading of existing, business information systems.

Note that:

- The principles set out in Part A of the Standard are valid for all electronic recordkeeping tools. Where this tool is a single system, that system should display all recommended features. Where multiple tools are used (e.g. shared drives, databases) each should incorporate the specific functionalities required for its particular tasks.
- The Standard will be supported by more specific products on related topics, to be issued by Archives New Zealand.

1.2 > SCOPE

Although the principles behind the functional specifications in this Standard apply to the management of records independent of the media in which they are stored, the specifications are primarily intended to guide the development and selection of electronic systems that ingest, maintain, and disseminate digital objects created by office automation systems and specialised systems. For example, digital objects created by e-mail, word processing, spreadsheet, and imaging applications (such as text documents, still and moving images, etc.), where they are of corporate value, should be managed within electronic recordkeeping systems that meet the functional specifications in this Standard.[1] Records controlled by an electronic recordkeeping system may be stored on a variety of different media, and be part of hybrid record aggregations which include both electronic and non-electronic elements.[2]

[1] See the following fact sheets from the *Continuum Resource Kit: What is a Corporate Record? (F/1)* and *Managing Government Records. Your Responsibility (F/7).*

[2] See Glossary (Section 5) for definitions of "aggregation" and "hybrid record".

The Standard does not include specifications for 'non-recordkeeping' functionality such as authentication, encryption, and integration with workflow applications. Nor does it include specifications for non-functional requirements common to all software applications such as the performance, scalability, and usability of the application. Though not included in this Standard's specifications, the importance of 'non-recordkeeping' and non-functional specifications to recordkeeping systems is noted by their inclusion in the high-level model in section 4.

Specifications for the long-term preservation of electronic records are omitted from the Standard as Archives New Zealand is currently undertaking work to identify appropriate electronic preservation methodologies for the New Zealand public sector. It is envisaged that guidance in this area will be issued in the future.

The specifications in this Standard will be cross-referenced to the recordkeeping metadata elements from the proposed Australasian Recordkeeping Metadata Standard once it is published.

1.3 > AUDIENCE

The intended audience of the Standard includes developers, vendors, purchasers and implementers of electronic recordkeeping systems - whether the systems are commercial off-the-shelf electronic recordkeeping software applications, or business information systems within which recordkeeping functionality is intended to be incorporated.

Accordingly, the language used in the Standard is intended to be as free from recordkeeping-specific terms as possible. Where this has not been possible, these terms have been defined in the glossary (section 5).

1.4 > STRUCTURE

The Standard is in two parts. Part A provides an overview of the Standard's conceptual basis and presents a high-level model of electronic recordkeeping functionality. The functional specifications are detailed in Part B, which forms the core of the Standard.

2 > RESPONSIBILITIES

This Standard is issued by the Chief Archivist to articulate best practice for recordkeeping across the New Zealand public sector. It is issued under the following sections of the Public Records Act 2005:

S17 requires every public office and local authority to create and maintain full and accurate records of its affairs, in accordance with normal, prudent business practice, and to maintain these records in an accessible form, until their disposal is authorised.

S27 empowers the Chief Archivist to issue standards for the creation, maintenance, or management of; appraisal for disposal of; and provision of access to public records or local authority records.

This standard applies to all public offices and local authorities subject to the Public Records Act 2005.

Compliance with this standard is discretionary.

3 > CONCEPTUAL BASIS

The *International Standard on Records Management (ISO 15489)*, endorsed by Archives New Zealand, defines records as "information created, received and maintained as evidence and information by an organisation or person in pursuance of legal obligation or in the transaction of business."[3]

ISO 15489 also states that records should be captured and managed within specialised business information systems called electronic recordkeeping systems.[4] A fundamental underlying principle is the distinction between business information systems and recordkeeping systems. Business information systems contain data that are constantly updated (timely), able to be transformed (manipulable) and only contain current data (non-redundant). By contrast, recordkeeping systems contain data that are explicitly linked to business activities (time-bound), unable to be altered (inviolable), and which may be non-current (redundant). Recordkeeping systems link records to business activities, retain records of past actions, and fix the content and structure of records.[5]

Archives New Zealand's *Recordkeeping Framework* provides a legislative and technologically neutral articulation of the key characteristics of recordkeeping systems.[6] This *Standard for Electronic Recordkeeping Systems* extends the *Framework* by defining a detailed set of functional specifications for electronic recordkeeping systems that support the *Framework's* principles within the New Zealand public sector's legislative and technological environment.

The generic requirements in the European Commission's *Model Requirements for the Management of Electronic Records: 'MoREQ' specification* form the basis for the Standard's functional requirements.[7]

4 > HIGH-LEVEL MODEL OF FUNCTIONAL SPECIFICATIONS

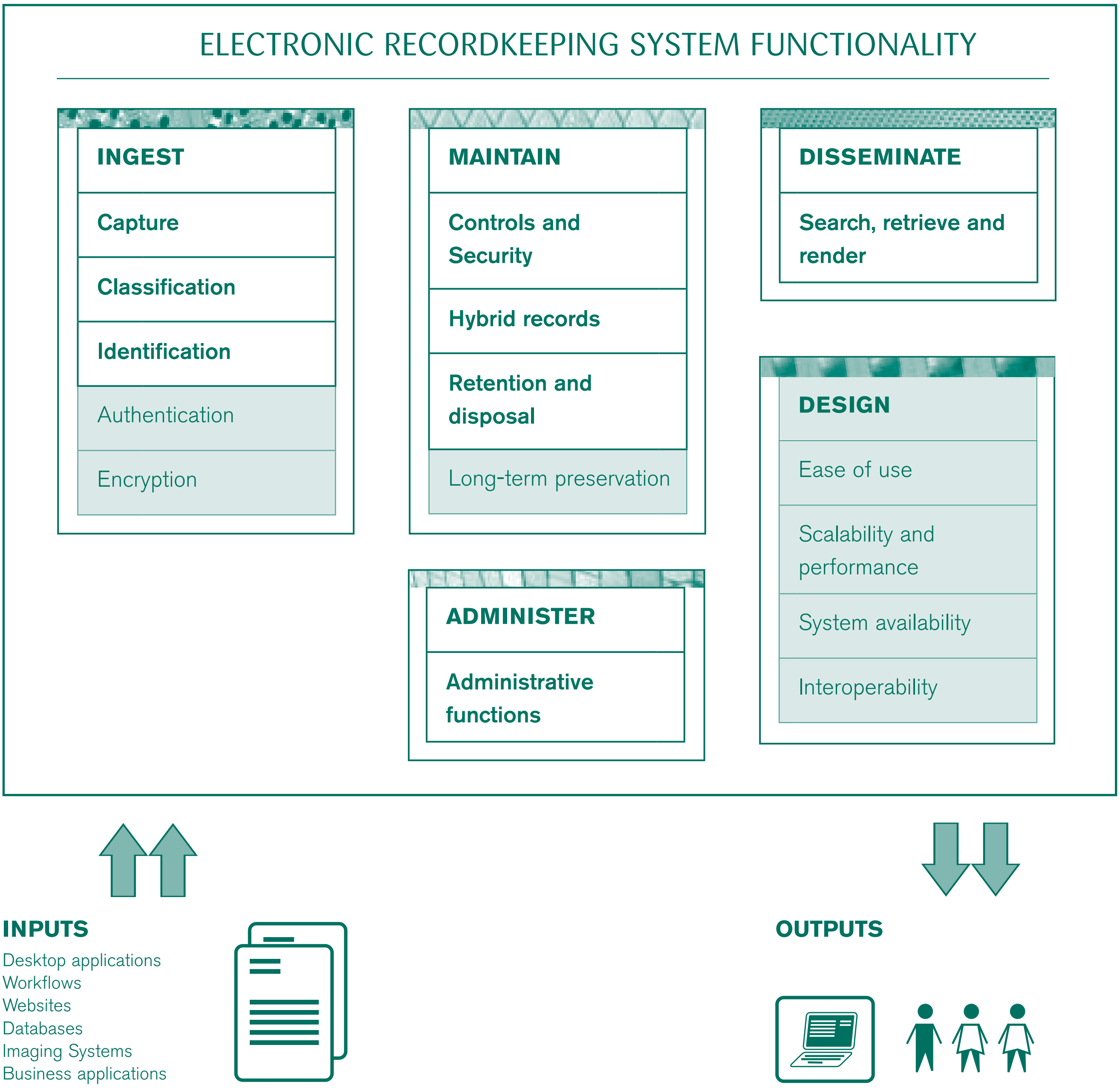
This section of the Standard identifies and briefly describes the functional specifications using a high-level model that clusters the specifications to highlight their interrelationships. The model is primarily intended to provide an 'at a glance' overview for users of the Standard who are not recordkeeping professionals.

Specifications for the long-term preservation of records, non-functional requirements common to all software applications, and 'non-recordkeeping' functionality are not detailed in the Standard but are indicated in the high-level model (solid green shading). Potential integration points with information technology architectures and other software applications are shown in the model as system inputs.

Individual specifications in Part B of this Standard are grouped according to the clusters from the high-level model in the following illustration.

[3] International Standards Organisation. 2001. *Information and documentation - Records management - Part 1* (ISO 15489), s3.15.
[4] *ISO 15489, Part1*, s3.17.
[5] Bearman, D. 1996. 'Item Level Control and Electronic Recordkeeping,' p.211.
[6] Archives New Zealand. 2000. *Recordkeeping Framework.*
[7] Cornwell Management Consultants plc. 2001. *Model requirements for the management of electronic records: 'MoREQ' specification.*

Figure 1. High-level model of functional specifications for electronic recordkeeping systems.[8]



ELECTRONIC RECORDKEEPING SYSTEM FUNCTIONALITY

INGEST
Capture
Classification
Identification
Authentication
Encryption

MAINTAIN
Controls and Security
Hybrid records
Retention and disposal
Long-term preservation

DISSEMINATE
Search, retrieve and render

DESIGN
Ease of use
Scalability and performance
System availability
Interoperability

ADMINISTER
Administrative functions

INPUTS
Desktop applications
Workflows
Websites
Databases
Imaging Systems
Business applications

OUTPUTS

Note 1: solid green shading indicates functionality not detailed in the Standard.

Note 2: the high-level model depicts the functional specifications that are the components of electronic recordkeeping systems. It does not depict the sequence of work processes that electronic recordkeeping systems perform.

[8] Thibodeau, K. 2001. 'Building the Archives of the Future. Advances in Preserving Electronic Records at the National Archives and Records Administration.' The Open Archival Information System (OAIS) reference model provides the underlying framework for this high-level model.

INGEST
Capture
Classification
Identification
Authentication
Encryption

4.1 > INGEST

Electronic recordkeeping systems uniquely capture, classify, and identify records in order to ensure that their content, structure, and context of creation is fixed in time and space. These recordkeeping processes, collectively referred to here as 'ingest', facilitate the making of complete, authentic, and usable records.[9]

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, e-mail, postal mail). Electronic recordkeeping systems must capture the content, structure and context of records in order to ensure they are reliable and authentic representations of the business activities or transactions in which they were created or transmitted.[10] Once captured within an electronic recordkeeping system, users should not be able to alter any of these features, although they should be able to create a new record by adding to the content, structure or context.

Classification

A classification scheme lies at the heart of any electronic recordkeeping system since it defines the way in which individual electronic records are grouped together (aggregated) and linked to the business context in which they were created or transmitted. By aggregating records, many of the recordkeeping processes described below can be carried out quickly and efficiently.

Agencies should take into account their own business needs when determining how records should be aggregated within their agency. For example, individual records in an agency-wide electronic recordkeeping system may be aggregated into files, and individual files, with their constituent records, may be subsequently aggregated into folders. (Note that these terms are indicative only. Different electronic recordkeeping systems employ different terminology.) Best practice aggregates records into three levels according to a three-tiered functional classification scheme as follows:[11]

Level 1.	Business Function
(aggregations of files - may be referred to as e.g. folders)	
Level 2.	Activity
(aggregations of individual records - may be referred to as e.g. files)	
Level 3.	Transaction

Note: 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.

[9] *Recordkeeping Framework*, principles 3.3, 3.7, and 3.8.
[10] Agency policy and procedures will determine when records should be captured into an electronic recordkeeping system.
[11] *ISO 15489, Part 1*, s3.5.

An electronic recordkeeping system that supports a single business activity (e.g. registration of companies) does not require a functional classification scheme but does require individual records to be aggregated in order to link them to their business context and to enable other recordkeeping processes.

Identification

In order to verify their existence within the system, every record and associated aggregation must have a unique identifier persistently linked to it.

MAINTAIN
Controls and Security
Hybrid records
Retention and disposal
Long-term preservation

4.2 > MAINTAIN

Records ingested into electronic recordkeeping systems must be actively maintained to ensure their continued accessibility. Establishing appropriate security controls, building in disposal outcomes, and enabling the management of hybrid records facilitates comprehensive, authentic, useable, tamper-proof and appropriately disposed records.[12]

Controls and security

Records captured into an electronic recordkeeping system must be protected against intentional or accidental alteration to their content, structure and context throughout their life to retain their authenticity. Audit trails, location tracking, access controls, and control over any alteration of records ensure the authenticity of records in an electronic recordkeeping system.

Organisations need to control access to their records. Typically, access to records and aggregations is limited to specific users and / or user groups. For the New Zealand public sector, access rights should be based on relevant provisions from the Public Records Act 2005, Official Information Act 1982, and the Privacy Act 1993, as well as agency-specific legislation.

In addition to controlling access by user and user groups, some agencies will need to limit access further by using the security classifications from the document *Security in the Government Sector.*[13] This is achieved by allocating security classifications to aggregations and / or records. Users can then be allocated security clearances to allow selective access to aggregations or records at higher security categories.

Maintaining an audit trail of all recordkeeping actions undertaken by an electronic recordkeeping system and its users and administrators is key to meeting requirements for legal admissibility. The volume of audit trail information can become large if all actions are audited. Consequently, in some implementations, management may decide that some actions need not be audited. In most cases, the online audit trail is periodically moved to offline storage and is disposed of at the same time as the records to which the audit trail relates.

Over time, records and aggregations may be transferred from one storage medium or location to another, as their activity decreases and / or their use changes. A tracking feature is needed to record the change of location for both ease of access and to meet regulatory requirements.

[12] *Recordkeeping Framework*, principles 3.4, 3.7, 3.8, 3.9 and 3.2.
[13] NZ Interdepartmental Committee on Security. June 2002. *Security in the Government Sector.* Chapter 3, Information Classification, pp.3.3-3.4

Retention and disposal

Disposal authorities are legal instruments issued under the Public Records Act 2005 to authorise the disposal of public records, whether by destruction or by transfer of control to the Chief Archivist (and possession by Archives New Zealand or an approved repository). Disposal authorities consist of disposal actions and agency retention periods for aggregations of records. Agencies should review disposal actions when the relevant retention periods have expired.

In addition to transfer of control under the Public Records Act 2005, records are transferred between electronic recordkeeping systems for a range of other reasons: for example, migration to a new electronic recordkeeping system as result of a technology refresh or an organisational restructuring. In all cases, whether required under the Public Records Act 2005 or not, transfer of records involves the movement of records to another electronic recordkeeping system and subsequent destruction of records from the original electronic recordkeeping system.[14] In all cases, the recordkeeping metadata and audit trails must be considered at the same time as the records to which they relate.

Hybrid record management

Agencies typically manage records that span a range of electronic and non-electronic media. Electronic recordkeeping systems must be able to ingest and maintain recordkeeping metadata relating to non-electronic records as well as electronic records and their associated recordkeeping metadata.

DISSEMINATE

Search, retrieve and render

4.3 > DISSEMINATE

An electronic recordkeeping system must be able to search for, retrieve and render the records that it maintains. These functions facilitate useable records.[15]

Search, retrieve and render

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

Rendering is the production of a human-readable representation of a record, usually to a display screen or in hard copy. Electronic recordkeeping systems typically contain records in a range of file formats. The user must be able to render records stored in these formats. Where it is meaningful to print a hard copy of a record the electronic recordkeeping system must provide functionality to allow all users to obtain printed copies of records and their recordkeeping metadata.[16]

[14] Note that the term transfer is used even though only a copy is sent to the other location or system.

[15] *Recordkeeping Framework*, principle 3.8.

[16] Sending screen image dumps to a printer is not normally considered acceptable for this requirement. Printing should be undertaken using the software application with all of the controls and features usually provided (such as multi-page reports, headings, use of any suitable configured printer).

ADMINISTER

Administrative functions

4.4 > 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. Administration facilitates useable records, reliable systems, systematic practices and the routine application of records management procedures.[17]

Administration

In exceptional circumstances, records may be altered or deleted by system administrators. Additionally, administrators will sometimes be required to release records as a result of Official Information Act requests where there is good reason for withholding some of the information contained in the records.[18]
Where this is the case, copies of the records without the sensitive information (redacted copies) must be able to be created. System administrators also need to be able to manage system parameters, back up and restore data, and generate system reports.

[17] *Recordkeeping Framework*, principles 3.8, 2.2, 2.3, and 2.5.
[18] Official Information Act 1982, s17. Deletion of information from documents.

5 > GLOSSARY

Although the language used in this Standard is intended to be as free from specialised terminology as is possible, the Standard does utilise a range of recordkeeping and information technology specific terms. For readers who are unfamiliar with these terms, they are defined in this section of the Standard.

Where definitions are based on other published sources, these are cited in abbreviated form at the end of each definition and full details provided in the Bibliography (section 6).

Term	Definition
Administrator	A role responsible for the day-to-day operation of the corporate recordkeeping policy within an organisation (MoReq). May also indicate responsibility for operation of the corporate recordkeeping system.
Aggregation	An ordered sequence of related records (MoReq). *Individual records may be aggregated into e.g. files, and individual files, with their constituent records, may be subsequently aggregated into e.g. folders (depending on terminology used by the electronic recordkeeping system in question).* See also Hybrid aggregation.
Application program interface (API)	An application program(ing) interface is the specific method prescribed by a computer operating system or application program so that the application program can make requests of the operating system or another application (Whatis.com).
Capture	The process of fixing the content, structure and context of a record to ensure that it is a reliable and authentic representation of the business activities or transactions in which it was created or transmitted. *Once captured within an electronic recordkeeping system, users should not be able to alter the content, structure and context of a record.*
Classification	The systematic identification and arrangement of business activities and / or records into categories according to logically structured conventions, methods, and procedural rules (ISO 15489).
Compound record	A record that comprises multiple individual electronic objects. *For example, web pages with embedded graphics and style sheets.*
Deletion	An information technology term for the process of eliminating a record from a system in such a way that the record may still be retrieved if necessary. Also known as 'soft delete'. See also Destruction.

Destruction	A recordkeeping term for the process of eliminating a record from a system beyond any possible reconstruction (ISO 15489). See also Deletion.
Disposal	The destruction, alteration, discharge, sale or transfer of control of a record (Public Records Act 2005). See also Destruction and Transfer.
Graphical User Interface (GUI)	A graphical, rather than purely textual, user interface to a computer (Whatis.com).
Hybrid record	A record consisting of electronic and non-electronic components (MoReq). *The electronic record and its associated recordkeeping metadata is maintained within the electronic recordkeeping system together with the recordkeeping metadata relating to the non-electronic record.*
Identification	The process of persistently linking a record or aggregation with a unique identifier.
Ingest	The recordkeeping processes that uniquely capture, classify, and identify records in order to ensure that their content, structure, and context of creation is fixed in time and space.
Record	Information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business (ISO 15489).
Record extract	A copy of a record to which some change has been applied to remove or mask but not to add to or meaningfully amend existing context (MoReq).
Recordkeeping metadata	Data that enables the creation, management, and use of records through time. Recordkeeping metadata can be used to identify, authenticate, and contextualise records as well as the people, processes and systems that create, manage, and maintain and use them (Archives New Zealand).
Redaction	The process of masking or deleting information in a record (MoReq).
Render	Rendering is the production of a human-readable representation of a record, usually to a display screen or in hard copy (MoReq).
Transfer	Used generally, refers to the transfer of records from one recordkeeping system to another and the subsequent destruction of records from the original electronic recordkeeping system. Used with reference to the Public Records Act 2005, refers to the transfer of control of records to the Chief Archivist, or to a public office that has taken over the recordkeeping responsibilities of a disestablished public office.
Volume	A sub-division of an electronic or non-electronic aggregation (MoReq). Also referred to as a "part". See also Aggregation.

Key to abbreviations for sources

Archives New Zealand	Archives New Zealand. *Glossary of Archives and Recordkeeping Terms.*
MoReq	Cornwell Management Consultants plc. *Model requirements for the management of electronic records: 'MoREQ' specification.*
ISO 15489	International Standards Organisation. *Information and documentation - Records management - Part 1.*
Whatis.com	Whatis.com information technology website.

6 > BIBLIOGRAPHY

Archives New Zealand. 2000. *Recordkeeping Framework (RK/1)*. Wellington, New Zealand: Archives New Zealand.

Archives New Zealand. 2003. *What is a Corporate Record? (F/1)*. Wellington, New Zealand: Archives New Zealand.

Archives New Zealand. 2003. *Glossary of Archives and Recordkeeping Terms (G/5)*. Wellington, New Zealand: Archives New Zealand.

Archives New Zealand. 2003. *Managing Government Records. Your Responsibility (F/7)*. Wellington, New Zealand: Archives New Zealand.

Bearman, D. 1996. 'Item Level Control and Electronic Recordkeeping.' *Archives and Museum Informatics* 10, No. 3: 195-245.

Bradner, S. 1997. RFC 2119: *Key words for use in RFCs to Indicate Requirement Levels*. www.faqs.org [Accessed 3 November 2003].

Cornwell Management Consultants plc. 2001. *Model requirements for the management of electronic records: 'MoREQ' specification*. www.cornwell.co.uk [Accessed 13 June 2003].

NZ Interdepartmental Committee on Security. June 2002. *Security in the Government Sector*. www.security.govt.nz [Accessed 17 December 2004].

International Standards Organisation. 1985. Documentation - *Guidelines for the establishment and development of multilingual thesauri. 5964:1985 (E)*. Geneva, Switzerland: International Standards Organisation.

International Standards Organisation. 1986. *Documentation - Guidelines for the establishment and development of monolingual thesauri. 2788:1986 (E)*. Geneva, Switzerland: International Standards Organisation.

International Standards Organisation. 2001. *Information and documentation - Records management - Part 1: Geneva. 15489-1:2001(E)*. Geneva, Switzerland: International Standards Organisation [ISO 15489, Part 1].

International Standards Organisation. 2001. *Information and documentation - Records management - Part 2: Guidelines. 15489-2:2001(E).* Geneva, Switzerland: International Standards Organisation [ISO 15489, Part 2].

UK Public Record Office. 2002. *Requirements for Electronic Records Management Systems: 1. Functional Requirements.* www.pro.gov.uk [Accessed 13 June 2003].

Thibodeau, K. 2001. 'Building the Archives of the Future. Advances in Preserving Electronic Records at the National Archives and Records Administration.' *D-Lib Magazine* 7, No. 2. www.dlib.org [Accessed 10 April 2003].

NZ State Services Commission, E-government Unit. July 2000. *New Zealand Government Data Management Standards, version 1.1.*

PART B: > FUNCTIONAL SPECIFICATIONS

Interpretation of functional specifications

Individual specifications in Part B of this Standard are grouped according to the clusters from the high-level model in Part A, section 4.

The keywords **'must'** and **'should'** that appear in the specifications in Part B indicate the relative importance of each specification. These keywords are to be interpreted as follows:[19]

Keyword	Interpretation
'must'	Specifications that use '**must**' are an absolute requirement for compliance with the Standard.
'should'	Specifications that use '**should**' may be ignored if a valid reason exists, but the full implications of ignoring the specification must be understood and carefully weighed before choosing a different course.

1 > CAPTURE

Capture Processes

The electronic recordkeeping system **must:**

1.1 provide an application programming interface (API) to enable integration with business applications so that transactional records created by the business applications can be captured within the electronic recordkeeping system.

1.2 indicate when an individual record is captured within the electronic recordkeeping system.

1.3 prevent the alteration of the content of any record by any user or administrator once it has been captured within the electronic recordkeeping system and has been certified as the final version (by whatever means this is done).

1.4 prevent the destruction or deletion of any record by any user, including an administrator, with the exceptions of:

- destruction in accordance with a disposal authority (see section 5 of this Part);
- deletion by an administrator (see section 8 of this Part).

1.5 support manual naming of electronic records, and allow this name to be different from the existing filename (including e-mail subject lines used to construct record titles). If the existing filename is taken by default, the electronic recordkeeping system must allow this name to be amended at the time of declaration.

[19] Bradner, S. 1997. *RFC 2119: Key words for use in RFCs to Indicate Requirement Levels.* These definitions in this Standard are based on the definitions from RFC 2119.

The electronic recordkeeping system **should:**

1.6 allow a user to pass electronic records to another user to complete the process of capture.

1.7 allow an administrator to un-register a captured record if required, to allow finalisation of the record profile. Any such temporary un-registration should be visible in an audit trail.

Recordkeeping Metadata

The electronic recordkeeping system **must:**

1.8 support the use of recordkeeping metadata for records.

1.9 acquire recordkeeping metadata elements for each record and persistently link them to the record over time (standard pending).[20]

1.10 ensure that the values for recordkeeping metadata elements conform to specified formats (standard pending).

1.11 allow the administrator to define (and re-define) the recordkeeping metadata elements associated with each record, including whether each element is mandatory or optional.

1.12 allow all recordkeeping metadata for every record to be viewed by users, subject to access rights for individuals or groups of users.

1.13 save the date and time of capture of each record as recordkeeping metadata elements linked to each record.

1.14 be capable of automatically extracting recordkeeping metadata from:

- the software application that created the record;
- the operating system;
- the electronic recordkeeping system.

1.15 prevent the alteration of recordkeeping metadata captured in specification 1.14.

1.16 allow entry of additional recordkeeping metadata by users during record capture and / or a later stage of processing by the user.

1.17 ensure that only authorised users and Administrators can change the content of those recordkeeping metadata elements captured in specification 1.16.

1.18 allocate an identifier, unique within the system, to each record at point of capture.

Aggregation

The electronic recordkeeping system **must:**

1.19 ensure that all records captured within the electronic recordkeeping system are associated with at least one aggregation.

1.20 manage the integrity of all pointers or references to records (where used), ensuring that:

- following a pointer, whichever aggregation that pointer is located in, will always result in correct retrieval of the record;
- change in location of a record also redirects any pointers which reference that record.

1.21 issue a warning if a user attempts to register a record that has already been registered in the same aggregation.

[20] Archives New Zealand is working with other archives and records authorities and professional bodies to develop an Australasian Recordkeeping Metadata Standard that will define required elements and specify the format in which they should be maintained.

1.22 not impose any practical limit on the number of records that can be captured in an aggregation, or on the number of records which can be stored in the electronic recordkeeping system. However, the system may permit limitations on the quantity of items within an aggregation if required for business purposes, e.g. to maintain parity between electronic and paper volumes.

1.23 allow users to choose at least one of the following where an electronic object has more than one version:

- register all versions of the object as one record;
- register one version of the object as a record;
- register each version of the object as a record.

The electronic recordkeeping system **should:**

1.24 support the ability to assign records to multiple aggregations without their duplication.

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 pointer system.

Bulk Importing

Records may be captured into an electronic recordkeeping system in bulk in a number of ways: for example, from another electronic recordkeeping system or as a bulk transfer from an electronic document management system or workflow application. The electronic recordkeeping system must be able to accept these, and must include features to manage the bulk capture process.

The electronic recordkeeping system **must:**

1.25 be able to capture in bulk records exported from other records management and document management systems, including capture of:

- electronic records in their existing format, without degradation of content or structure, retaining the relationship between the components of any individual record;
- electronic records and all associated recordkeeping metadata, retaining the correct relationship between individual records and their metadata attributes;
- the structure of aggregations to which the records are assigned, and all associated recordkeeping metadata, retaining the correct relationship between records and aggregations.

The electronic recordkeeping system **should:**

1.26 be able to import any directly associated audit information with the record and/or aggregation, retaining this securely within the imported structure.

Document Types

The electronic recordkeeping system **must:**

1.27 allow users to capture and store records in their native format.

1.28 support the capture of records created in file formats from the following commonly used software applications:

- standard office applications (word processing, spread-sheeting, presentation, simple databases);

- e-mail client applications;
- imaging applications;
- web authoring tools.

1.29 be able to extend the range of file formats supported for specification 1.28 as new file formats are introduced.

1.30 capture compound electronic records (records comprising more than one component) so that:

- the relationship between the constituent components of each compound record is retained;
- the structural integrity of each compound record is retained;
- each compound record is retrieved, displayed, and managed as a single unit;
- each compound record is disposed of as a single unit.

1.31 be able to ingest such compound records easily, preferably with one action, e.g. a single click.

Where agencies have implemented specialised software applications to manage architectural, financial, geospatial, personnel, or statistical data, the electronic recordkeeping system **should:**

1.32 support the capture of records created in the file formats from these applications.

E-mail

E-mail is used for sending both simple messages and documents (as attachments), within and between organisations. The characteristics of e-mail can make it difficult to track and register. Agencies must provide users with the capability of capturing selected e-mail messages and attachments.

The electronic recordkeeping system **must:**

1.33 allow users to capture e-mails (text and attachments) as single records.

1.34 allow individual users to capture e-mail messages (and attachments) from within their e-mail application.

1.35 allow users to choose whether to capture e-mails with attachments as:

- e-mail text only;
- e-mail text with attachments;
- attachments only.

1.36 ensure the capture of e-mail transmission data as recordkeeping metadata persistently linked to the e-mail record.

1.37 ensure that the text of an e-mail and its transmission details cannot be amended in any way once the e-mail has been captured. Nor should the subject line of the e-mail itself be changeable, although the title of the record may be edited for easier access through e.g. keywords.

1.38 ensure that a human-readable version of an e-mail message address is also captured, where one exists.

For example, for ***"Joe McClaine" <joe90@worldintnet.org>,*** *"Joe McClaine" is the human-readable version of the e-mail address joe90@worldintnet.org.*

2 > CLASSIFICATION

Establishing a Classification Scheme

The electronic recordkeeping system **must:**

2.1 support and be compatible with the agency's classification scheme.

2.2 be able to support a classification scheme which can represent aggregations as being organised in a hierarchy with a minimum of three levels.

2.3 allow naming conventions to be defined at the time the electronic recordkeeping system is configured.

2.4 support the initial construction of a classification scheme at the time the electronic recordkeeping system is configured, in readiness for the capture or importation of electronic records.

2.5 allow Administrators to create aggregations at any level within any aggregation.

2.6 not limit the number of levels in the classification scheme hierarchy.

The electronic recordkeeping system **should:**

2.7 support the definition and simultaneous use of multiple classification schemes.

This may be required, for example, following the merger of two organisations. It is not intended for routine use.

2.8 support a distributed classification scheme that can be maintained across a network of electronic record repositories.

Where the electronic recordkeeping system employs a graphical user interface (GUI), it **must:**

2.9 support browsing and graphical navigation of the aggregations and classification scheme structure and the selection, retrieval and display of electronic aggregations and their contents through this mechanism.

Aggregations

The electronic recordkeeping system **must:**

2.10 support recordkeeping metadata for aggregations in the classification scheme.

2.11 provide at least two naming mechanisms for electronic aggregations in the classification scheme:

- a mechanism for allocating a structured numeric or alphanumeric reference code (i.e. an identifier which is unique within the classification scheme) to each electronic aggregation;
- a mechanism to allocate a textual title for each electronic aggregation.
- It must be possible to apply both identifiers separately or together.

2.12 allow only Administrators to create new aggregations at the highest level in the classification scheme (for example, at the business function level).

2.13 record the date of opening of a new aggregation within the recordkeeping metadata associated with it.

2.14 automatically include in the recordkeeping metadata of each new aggregation those attributes that derive from its position in the classification scheme (e.g. name, classification code).

For example, if a "Correspondence" file is in a hierarchical path: "Regional plan development : Public consultation : Correspondence" and the Administrator adds a new file named "Formal Objections" at the same level as the

"Correspondence" file then it must automatically inherit the prefix "Regional plan development : Public consultation."

2.15 not impose any practical limit on the number of aggregations that can be defined.

2.16 allow the automatic creation and maintenance of a list of aggregations.

The electronic recordkeeping system **should**:

2.17 support an optional aggregation 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 the linking of the thesaurus to the classification scheme.

2.18 support an optional aggregation naming mechanism that includes names (e.g. persons' names) and / or dates (e.g. dates of birth) as file names, including validation of the names against a list.

2.19 support the allocation of controlled vocabulary terms compliant to ISO 2788 or ISO 5964 as recordkeeping metadata, in addition to the other requirements in this section.

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 specifications for volumes only apply to the aggregations at the activity level.

Where the electronic recordkeeping system uses volumes, it **must**:

2.20 allow Administrators to add (open) electronic volumes to any electronic aggregation that is not closed.

2.21 record the date of opening of a new volume in the volume's recordkeeping metadata.

2.22 automatically include in the metadata of new volumes those attributes of its parent aggregation's recordkeeping metadata which are common (e.g. name, classification code).

2.23 support the concept of open and closed volumes for electronic aggregations, as follows:

- only the most recently created volume within an aggregation can be open;
- all other volumes within that aggregation must be closed (subject to temporary exceptions required by specification 2.25).

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

2.24 prevent the user from adding electronic records to a closed volume (subject to the exceptions required by specification 2.25).

2.25 allow an Administrator to re-open a previously closed volume temporarily for the addition of records, and subsequently to close that volume again.

This facility is intended to be used to rectify user error, e.g. if a volume has been closed unintentionally.

Maintaining the Classification Scheme

The electronic recordkeeping system **must:**

2.26 allow an electronic aggregation (including volumes) to be relocated to a different position in the classification scheme, and must ensure that all electronic records already allocated remain allocated to the aggregations (including volumes) being relocated.

This facility is intended for exceptional circumstances only, such as organisational mergers or other re-organisation, or to *correct clerical errors. This requirement must be read together with specifications 2.28, 2.29, and 2.37.*

2.27 allow an electronic record to be re-classified to a different volume of an electronic aggregation.

This facility is intended for exceptional circumstances only, such as to correct clerical errors. This requirement must be read together with specifications 2.28, 2.29, and 2.37.

2.28 restrict to Administrators the ability to move aggregations (including volumes) and individual records.

2.29 keep a clear trace of the status of reclassified aggregations (including volumes) prior to their reclassification, so that their entire history can be determined easily.

At a minimum, this must be stored in the audit trail. It may also be desirable to record it elsewhere, e.g. in the recordkeeping metadata of the object(s) being moved.

2.30 prevent the deletion of an electronic aggregation or any part of its contents at all times, with the exceptions of:

- destruction in accordance with a disposal authority;
- deletion by an Administrator as part of an audited procedure.

2.31 allow an electronic aggregation to be closed by a specific Administrator procedure, and must restrict this function to an Administrator.

2.32 record the date of closing of a volume in the volume's recordkeeping metadata.

2.33 maintain internal integrity (relational integrity or otherwise) at all times, regardless of:

- maintenance activities;
- other user actions;
- failure of system components.

In other words, it must be impossible for a situation to arise where any user action or any software failure results in an inconsistency within the electronic recordkeeping system or its database.

2.34 not allow any volume that has been temporarily re-opened (as in specification 2.25) to remain open after the Administrator who opened it has logged off.

2.35 allow users to create cross-references between related aggregations or between aggregations and individual records.

2.36 provide reporting tools for the provision of statistics to the Administrator on aspects of activity within the classification scheme, including the numbers of electronic aggregations (including volumes) or records created, closed or deleted within a given period.

The electronic recordkeeping system **should:**

2.37 allow the Administrator to enter the reason for the reclassification of aggregations (including volumes) and individual records.

2.38 be able to close a volume of an electronic aggregation automatically on fulfilment of specified criteria to be defined at configuration, including at least:

- volumes delineated by an annual cut-off date (e.g. end of the calendar year, financial year or other defined annual cycle);

- the passage of time since a specified event (e.g. the most recent addition of an electronic record to that volume);
- the number of electronic records within a volume.

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

3 > IDENTIFICATION

The electronic recordkeeping system **must:**

3.1 associate each of the following with a unique identifier:

- Record;
- Record extract;
- Aggregation (including volume).

3.2 require all unique identifiers to be unique, either:

- within the entire electronic recordkeeping system; or
- within the aggregation within which the record entity appears.

3.3 be able to store the unique identifiers as recordkeeping metadata elements of the entities to which they refer.

3.4 either:

- generate unique identifiers automatically and prevent users from inputting the unique identifier manually, and from subsequently modifying it (for example, a sequential number); or
- allow users to input a unique identifier, but validate that it is unique before it is accepted (for example, an account number).

3.5 allow the format of the unique identifier to be specified at configuration time.

The identifier may be a number or alphanumeric, or may include the concatenated identifiers of the volume and electronic aggregations above the record in the classification scheme.

Where unique identifiers are automatically generated, the electronic recordkeeping system **should:**

3.6 allow the Administrator to specify at configuration time the starting number (e.g. 1, 10, 100) and increment (e.g. 1, 10) to be used in all cases.

Where the unique identifiers are based on sequential numbering, the electronic recordkeeping system **should:**

3.7 automatically generate the next sequential number available at that position within the classification scheme for each new electronic aggregation.

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

then if the Administrator adds a new aggregation to the 'Order Processing' aggregation, the electronic recordkeeping system should automatically assign it the reference 900 - 23 - 04. Likewise, if the Administrator adds a new class to the 'Manufacturing' aggregation the electronic recordkeeping system should automatically assign it the reference 900 - 24.

4 > CONTROLS AND SECURITY

Access

The electronic recordkeeping system **must:**

4.1 allow the Administrator to limit access to records, aggregations and recordkeeping metadata to specified users or user groups.

4.2 allow the Administrator to attach to the user profile attributes which determine the features, recordkeeping metadata fields, records or aggregations to which the user has access. The attributes of the profile will:

- prohibit access to the electronic recordkeeping system without an accepted authentication mechanism attributed to the user profile;
- restrict user access to specific records or aggregations;
- restrict user access according to the user's security clearance;
- restrict users access to particular features (e.g. read, update and / or delete specific recordkeeping metadata fields);
- deny access after a specified date;
- allocate the user to a group or groups.

An example of an accepted authentication mechanism is
a password.

4.3 be able to provide the same control functions for roles as for users.

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, Database Administrator.

4.4 be able to set up groups of users that are associated with an aggregation.

Examples of groups might be Personnel, or Sales team.

4.5 allow a user to be a member of more than one group.

4.6 allow only Administrators to set up user profiles and allocate users to groups.

4.7 allow changes to security attributes for groups or users (such as access rights, security level, privileges, password allocation and management) to be made only by the Administrator.

4.8 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:

- display title and recordkeeping metadata;
- display the existence of an aggregation or record (i.e. display its file or record number) but not its title or other recordkeeping metadata;
- do not display any record information or indicate its existence in any way.

These options are presented in order of increasing security. Note that the requirement in the third option (i.e. the most stringent) implies that the electronic recordkeeping system must not include such records in any count of search results.

4.9 never include, in a list of full text or other search results, any record which the user does not have the right to access.

Note that if the first option of requirement specification 4.8 is chosen, specification 4.9 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.

If the electronic recordkeeping system allows users to make unauthorised attempts to access aggregations (and their volumes) or records, the electronic recordkeeping system **must:**

4.10 log all unauthorised attempts to access aggregations (and their volumes) or records in their respective audit trails.

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

If the electronic recordkeeping system maintains an list of aggregations, the electronic recordkeeping system **must:**

4.11 be able to limit users' access to parts of the list (to be specified at the time of configuration).

The electronic recordkeeping system **should**:

4.12 allow a user to stipulate which other users or groups can access records that the user is responsible for.

This function should be granted to the user by the Administrator according to the agency's policy.

Audit Trails

The electronic recordkeeping system ***must:***

4.13 be capable of creating an unalterable audit trail of recordkeeping actions (actions to be specified by each agency) that are taken upon records, aggregations, or the classification scheme. The audit trail should include the following recordkeeping metadata elements:

- type of recordkeeping action;
- user initiating and/or carrying out the action;
- date and time of action.

The word "unalterable" is to mean that the audit trail data cannot be modified in any way or deleted by any user; it may be subject to re-organisation and copying to removable media if required by, for example, database software, so long as its content remains unchanged.

4.14 track events, once the audit trail functionality has been activated, without manual intervention, and store in the audit trail information about them.

4.15 maintain the audit trail for as long as required.

4.16 provide an audit trail of all changes made to:

- electronic aggregations (including volumes);
- individual electronic records;
- recordkeeping metadata associated with any of the above.

4.17 provide an audit trail of all changes made to administrative parameters (for example, changes made by the Administrator to a user's access rights).

4.18 be capable of capturing and storing in the audit trail information about the following actions:

- the date and time of capture of all electronic records;
- re-classification of an electronic record in another electronic volume;
- re-classification of an electronic aggregation in the classification scheme;
- any change to the disposal authority of an electronic aggregation;
- any change made to any recordkeeping metadata associated with aggregations or electronic records;
- date and time of creation, amendment and deletion of recordkeeping metadata;
- changes made to the access privileges affecting an electronic aggregation, electronic record or user;
- export or transfer actions carried out on an electronic aggregation;
- date and time at which a record is rendered;
- disposal actions on a electronic aggregation or record.

4.19 ensure that audit trail data is available for inspection on request, so that a specific event can be identified and all related data made accessible, and that this can be achieved by authorised external personnel who have little or no familiarity with the system.

4.20 be able to export audit trails for specified records and selected groups of records without affecting the audit trail stored by the electronic recordkeeping system.

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

4.21 be able to capture and store violations (i.e. a user's attempts to access a record or aggregation, including volumes, to which he or she is denied access), and (where violations can validly be attempted) attempted violations, of access control mechanisms.

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

4.22 be able, at a minimum, to provide reports for actions on records and aggregations organised:

- by record or aggregation;
- by user;
- in chronological sequence.

The electronic recordkeeping system **should:**

4.23 allow the audit trail facility to be configurable by the Administrator so that the functions for which information is automatically stored can be selected. The electronic recordkeeping system must ensure that this selection and all changes to it are stored in the audit trail.

4.24 be able to provide reports for actions on aggregations and records organised by workstation and (where technically appropriate) by network address.

Backup and Recovery

Electronic recordkeeping systems must have comprehensive controls to create regular backups of the records and recordkeeping metadata that they maintain. These backups should enable the electronic recordkeeping system to rapidly recover records if any are lost because of system failure, accident, or security breach. In practice, backup and recovery functions may be divided between electronic recordkeeping system administrators and information technology staff.

The electronic recordkeeping system **must:**

4.25 provide automated backup and recovery procedures that allow for regular backup of all or selected classes, aggregations, records, recordkeeping metadata and administrative attributes of the electronic recordkeeping system repository.

4.26 allow the Administrator to schedule backup routines by:

- specifying the frequency of backup;
- selecting classes, aggregations or records to be backed up;
- allocating storage media, system or location for the backup (e.g. offline storage, separate system, remote site).

4.27 allow only the Administrator to restore from electronic recordkeeping system backups. Full integrity of the data must be maintained after restoration.

4.28 allow only the Administrator to roll-forward the electronic recordkeeping system from a backup to a more recent state, maintaining full integrity of the data.

4.29 allow users to indicate that selected records are considered to be 'vital records'.

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

The electronic recordkeeping system **should:**

4.30 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.

4.31 allow vital records and other records to be restored in distinct operations.

Tracking Record Movement

The electronic recordkeeping system **must:**

4.32 provide a tracking feature to monitor and record information about the location and movement of both electronic and non-electronic aggregations.

4.33 record information about movements including:

- unique identifier of the aggregation or record;
- current location as well as a user-defined number of previous locations (locations should be user-defined);
- date item sent/moved from location;
- date item received at location (for transfers);
- user responsible for the move (where appropriate).

4.34 maintain access to the electronic record content, including the ability to render it, and maintenance of its structure and formatting, over time and through generations of office application software.

This may be, but does not have to be, by use of a multi-format viewer application.

Authenticity

The electronic recordkeeping system **must:**

4.35 restrict access to system functions according to user's role and strict system administration controls.

4.36 be able, where possible and appropriate, to provide a warning if an attempt is made to capture a record which is incomplete or inconsistent in a way which will compromise its future apparent authenticity.

For example, a purchase order without a valid electronic signature, or an invoice from an unrecognised supplier.

4.37 prevent any unrecorded change to the content of the electronic record by users and Administrators.

Security Categories

The specifications in this section only apply to agencies that are managing classified records within their electronic recordkeeping system.

The electronic recordkeeping system **must:**

4.38 allow security classifications to be assigned to records.

4.39 allow one of the following to be selected at configuration time:

- security classifications to be assigned to aggregations (including volumes) and records;
- security classifications to be assigned to individual records.

4.40 allow one of the following security clearances to be assigned to users:[21]

- Unclassified;
- In Confidence (policy and privacy);
- Sensitive (policy and privacy);
- Restricted (national security information);
- Confidential (national security information);
- Secret (national security information);
- Top Secret (national security information).

4.41 deny users access to electronic records that have a security classification higher than their security clearance.

[21] *Security in the Government Sector.* Chapter 3.

Note that the correct level of security clearance may not be sufficient to obtain access. Access to the electronic records may in addition be restricted to specified users, roles and / or groups.

4.42 support the automated application of a default value of 'Unclassified' to an aggregation or record not allocated any other security category.

The electronic recordkeeping system **should**:

4.43 enable its security subsystem to work effectively together with general security products.

4.44 be able to determine the highest security category of any record in any aggregation by means of one simple enquiry.

4.45 support routine, scheduled reviews of security classifications.

If security classifications are assigned to aggregations as well as individual records (as per specification 4.39), then the electronic recordkeeping system **must:**

4.46 deny users access to aggregations that have a security classification higher than their security clearance.

Note that the correct level of security clearance may not be sufficient to obtain access. Access to the electronic records may in addition be restricted to specified users, roles and / or groups.

If security classifications are assigned to aggregations as well as individual records (as per specification 4.39), then the electronic recordkeeping system **should:**

4.47 be capable of preventing an electronic aggregation from having a lower security classification than any electronic record within that aggregation.

5 > RETENTION AND DISPOSAL

Disposal Authorities

The electronic recordkeeping system **must:**

5.1 provide a function that:

- specifies disposal authorities;
- automates reporting and destruction actions; and
- provides integrated facilities for exporting records and recordkeeping metadata.

5.2 be able to restrict the setting up and changing of disposal authorities to the Administrator only.

5.3 allow the Administrator to define and store a standard set of customised standard disposal authorities.

5.4 be capable of assigning a disposal authority to any record or aggregation.

5.5 by default, ensure that every record in an aggregation is governed by the disposal authority(s) associated with that aggregation.

5.6 include a disposal action (specification 5.8), agency retention period (specification 5.9), and disposal authority number for the decision for each disposal authority.

5.7 for each aggregation:

- automatically track retention periods that have been allocated to the aggregation;
- initiate the disposal process once the end of the retention period is reached.

5.8 allow at least the following decisions for each disposal authority:

- retain indefinitely;
- present for review at a future date (date defined as per specification 5.9);

- destroy at a future date (date defined as per specification 5.9);
- transfer at a future date (date defined as per specification 5.9).

5.9 allow retention periods for each disposal authority (as defined in specification 5.8) to be specified for a future date, with the date able to be set in at least the following ways:

- passage of a given period of time after the aggregation is opened;
- passage of a given period of time after the aggregation is closed;
- passage of a given period of time since the most recent record has been assigned to the aggregation;
- passage of a given period of time after a specific event (event to be identified in the schedule, and will be notified to the electronic recordkeeping system by the Administrator rather than being detected automatically by the electronic recordkeeping system);
- specified as "indefinite" to indicate long-term preservation of the records.

While the above is generally inclusive, it is possible that some records will have types of retention requirements which are not listed here.

5.10 support retention periods (as per specification 5.9) from a minimum of one month to an indefinite period.

5.11 automatically record and report all disposal actions to the Administrator.

5.12 enable a disposal authority to be assigned to an aggregation that over-rides the disposal authority assigned to its 'parent' aggregation.

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

5.13 allow the Administrator to amend any disposal authority allocated to any aggregation at any point in the life of that aggregation.

5.14 allow the Administrator to change the authority(s) associated with an aggregation at any time.

The electronic recordkeeping system **should:**

5.15 be capable of associating more than one disposal authority with any aggregation or class of a classification scheme.

For example, an aggregation may have one schedule which is the standard schedule for the organisation it belongs to, and a second schedule which is a special schedule related to litigation that is specific to this aggregation.

5.16 allow the definition of sets of processing rules that can be applied as an alerting facility to specified aggregations prior to initiation of a disposal process.

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.

5.17 provide the option of allowing electronic records or aggregations that are being moved between aggregations by the Administrator to have the disposal authority of the new aggregation, replacing the existing disposal authority(s) applying to these records.

If more than one disposal authority is associated with an aggregation, the electronic recordkeeping system **must:**

5.18 automatically track all retention periods specified in these disposal authorities, and initiate the disposal process once the last of all these retention dates is reached.

Reviewing

The electronic recordkeeping system **must:**

5.19 support the review process by presenting electronic aggregations to be reviewed, with their recordkeeping metadata and disposal authority information, in a manner that allows the reviewer to browse the contents of the aggregation and / or recordkeeping metadata efficiently.

5.20 allow the reviewer to take <u>at least</u> any one of the following actions for each aggregation during review:

- mark the aggregation for destruction;
- mark the aggregation for transfer (see specification 5.35);
- change the disposal authority (or assign a different schedule) so that the aggregation is retained and re-reviewed at a later date, the date to be defined as in specification 5.9.

5.21 allow the reviewer to enter comments into the aggregation's recordkeeping metadata to record the reasons for the review decisions.

5.22 alert the Administrator to aggregations due for disposal before implementing disposal actions; and on confirmation from the Administrator the electronic recordkeeping system must be capable of initiating the disposal actions specified in specification 5.8.

5.23 store in the audit trail all decisions taken by the reviewer during reviews.

The electronic recordkeeping system **should:**

5.24 produce a disposal authority report for the Administrator that identifies all disposal authorities that are due to be applied in a specified time period, and provide quantitative reports on the quantity and types of records covered.

5.25 be able to specify the frequency of a disposal authority report, the information reported and highlight exceptions such as overdue disposal.

5.26 alert the Administrator if an electronic 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:

- confirmation by the Administrator to proceed with or cancel the process;
- generation of a report detailing the aggregation or record(s) concerned and all references or links for which it is a destination.

5.27 support reporting and analysis tools for the management of retention and disposal authorities by the Administrator, including the ability to:

- list all disposal authorities;
- list all electronic aggregations to which a specified disposal authority is assigned;
- list the disposal authority(s) applied to all aggregations below a specified point in the hierarchy of the classification scheme;
- identify, compare and review disposal authorities (including their contents) across the classification scheme;
- identify formal contradictions in disposal authorities across the classification scheme.

5.28 provide, or support the ability to interface with, a workflow facility to support the scheduling, review and export / transfer process, by tracking:

- progress / status of the review, such as awaiting or in-progress, details of reviewer and date;
- records awaiting disposal as a result of a review decision;
- progress of the transfer process.

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

Transfer, Export and Destruction

The electronic recordkeeping system **must:**

5.30 provide a well-managed process to transfer records to another system or to a third party organisation.

5.31 include all aggregations, volumes, records and associated recordkeeping metadata within aggregations whenever an electronic recordkeeping system transfers any aggregation or volume.

5.32 be able to transfer or export an aggregation (at any level) in one sequence of operations so that:

- the content and structure of its electronic records are not degraded;
- all components of an electronic record (when the record consists of more than one component) are exported as an integral unit;
- all links between the record and its recordkeeping metadata are retained;
- all links between electronic records, volumes and aggregations are retained.

5.33 be able to include a copy of all the audit trail data associated with the records, volumes and aggregations that are transferred or exported from an electronic recordkeeping system.

5.34 produce a report detailing any failure during a transfer, export or destruction. The report must identify any records destined for transfer that have generated processing errors, and any aggregations or records which are not successfully transferred, exported or destroyed.

5.35 retain copies of all electronic aggregations and their records which have been transferred, at least until such time as a successful transfer is confirmed.

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

5.36 be able to continue to manage records and aggregations that have been exported from the electronic recordkeeping system to other forms of storage media.

5.37 have the ability to retain recordkeeping metadata for records and aggregations that have been destroyed or transferred.

5.38 allow the Administrator to specify a subset of aggregation recordkeeping metadata which will be retained for aggregations which are destroyed, transferred out or moved offline.

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 recordkeeping metadata for the records.

The electronic recordkeeping system **should:**

5.39 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.

5.40 provide the ability to add user-defined recordkeeping metadata elements required for archival management purposes to electronic aggregations selected for transfer.

5.41 provide the ability to sort electronic aggregations selected for transfer into ordered lists according to user-selected recordkeeping metadata elements.

5.42 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 by use of specialist data recovery facilities.

Where hybrid aggregations are to be transferred, exported or destroyed, the electronic recordkeeping system **should:**

5.43 require the Administrator to confirm that the paper part of the same aggregations has been transferred, exported or destroyed before transferring, exporting or destroying the electronic part.

6 > HYBRID RECORD MANAGEMENT

Management of Electronic and Non-electronic Records

The electronic recordkeeping system **must:**

6.1 be able to define in the classification scheme non-electronic aggregations and volumes, and must allow the presence of non-electronic records in these volumes to be reflected and managed in the same way as electronic records.

6.2 define in the classification scheme aggregations which (logically) contain both electronic and non-electronic records, and must allow both kinds of record to be managed in an integrated manner.

These files are referred to as "hybrid aggregations" in this specification. In practice, hybrid aggregations will consist of both electronic and non-electronic components.

6.3 allow a non-electronic aggregation that is associated as a hybrid with an electronic aggregation to use the same title and numerical reference code, but with an added indication that it is a hybrid non-electronic aggregation.

6.4 allow a different recordkeeping metadata element set to be configured for non-electronic and electronic aggregations; non-electronic aggregation recordkeeping metadata must include information on the physical location of the non-electronic aggregation.

6.5 ensure that retrieval of non-electronic aggregations displays the recordkeeping metadata for both electronic and non-electronic records associated with it.

6.6 include features to control and record access to non-electronic aggregations, including controls based on security category, which are comparable to the features for electronic aggregations.

6.7 support tracking of non-electronic aggregations by the provision of request, check-out, and check-in facilities which reflect the current location of the item concerned.

The electronic recordkeeping system **should:**

6.8 support the printing and recognition of bar codes for non-electronic objects (e.g. documents, folders and other containers), or should support other tracking systems to automate the data entry for tracking the movement of such non-electronic records.

Where aggregations have security categories, the electronic recordkeeping system **must:**

6.9 ensure that a hybrid non-electronic aggregation is allocated the same security category as an associated hybrid electronic aggregation.

Retention and Disposal of Electronic and Non-electronic Records

The electronic recordkeeping system **must:**

6.10 support the allocation of disposal authorities to every non-electronic aggregation in the classification scheme. The authorities must function consistently for electronic and non-electronic aggregations, notifying the Administrator when the disposal date is reached, but taking account of the different processes for disposing of electronic and non-electronic records.

6.11 support the application of the same disposal authority to both the electronic and non-electronic aggregations that make up a hybrid aggregation.

6.12 be able to apply any review decision made on a hybrid electronic aggregation to a non-electronic aggregation with which it is associated.

6.13 alert the Administrator to the existence and location of any hybrid non-electronic aggregation associated with a hybrid electronic aggregation that is to be exported or transferred.

6.14 be able to record in the audit trail all changes made to recordkeeping metadata references to non-electronic or hybrid aggregations and records.

The electronic recordkeeping system **should:**

6.15 support the application of a review decision taken on a group of aggregations to any non-electronic aggregations within that group, by notifying the Administrator of necessary actions to be taken on the non-electronic aggregations.

6.16 be able to export and transfer recordkeeping metadata of non-electronic records and aggregations.

6.17 be capable of offering check-out and check-in facilities for non-electronic aggregations profiled in the system, in particular enabling the ability to record a specific user or location to which a non-electronic aggregation is checked-out, and to display this information if the non-electronic aggregation is requested by another user.

6.18 be capable of offering a request facility for non-electronic aggregations profiled in the system, enabling a user to enter a date that the non-electronic aggregation is required, and generating a consequent message for transmission to the current holder of that non-electronic aggregation or the Administrator, according to configuration.

7 > SEARCH, RETRIEVE AND RENDER

Note that the electronic recordkeeping systems must never present information to any user who is not entitled to access it. All the features and functionality in this section must be subject to access controls as described in section 4. To avoid complexity, this is assumed and is not repeated in each detailed requirement.

General

The electronic recordkeeping system **must:**

7.1 provide a flexible range of functions that operate on the recordkeeping 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 recordkeeping metadata.

7.2 allow all record, volume and aggregation recordkeeping metadata to be searchable.

7.3 allow the text contents of records (where they exist) to be searchable.

7.4 allow the user to set up a single search request with combinations of recordkeeping metadata and / or record content.

7.5 allow Administrators to configure and change the search fields to:

- specify any element of record, volume and aggregation recordkeeping metadata, and optionally full record content, as search fields;
- change the search field configuration.

7.6 provide searching tools that cover the following techniques:

- free-text searching of combinations of record and aggregation recordkeeping metadata elements and record content;

- boolean searching of recordkeeping metadata elements.

7.7 provide for "wild card" searching of recordkeeping metadata that allows for forward, backward and embedded expansion.

For example, the search term 'proj' might retrieve 'project' or 'PROJA'; the term 'C*n' would retrieve 'Commission'.*

7.8 allow searching within a single aggregation or across more than one aggregation.

7.9 be able to search for, retrieve, and display all the records and recordkeeping metadata relating to an electronic aggregation, or volume, as a single unit.

7.10 be able to search for, retrieve and render an electronic aggregation by all implemented naming principles, including:

- name;
- identifier (classification code).

7.11 display the total number of search results on the user's screen and must allow the user to then display the results list, or refine the search criteria and issue another request.

7.12 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.

7.13 allow users to retrieve aggregations and records directly through use of a unique identifier.

7.14 never allow a search or retrieval function to reveal to a user any information (recordkeeping metadata or record content) which the access and security settings are intended to hide from that user.

The electronic recordkeeping system **should:**

7.15 have integrated search facilities that appear the same to users for all levels of the classification scheme.

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

7.16 present seamless functionality when searching across electronic, non-electronic, and hybrid aggregations.

7.17 provide free-text and recordkeeping metadata searches in an integrated and consistent manner.

7.18 provide concept searches through the use of a thesaurus incorporated as an online index.

This will allow retrieval of documents with a broader, narrower, or related term in their content or recordkeeping metadata. For example, a search for "ophthalmic services" might retrieve "health services", "eye test" or "ophthalmology".

7.19 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.

7.20 allow the recordkeeping metadata of any object (such as record, volume, or aggregation) to be searched, whether the object itself is in electronic form or not, and regardless of whether the object is stored online, near-line or offline.

7.21 allow users to save and re-use queries.

7.22 allow users to refine (i.e. narrow) searches.

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.

7.23 provide display formats configurable by users or Administrators for search results, including such features and functions as:

- select the order in which the search results are presented;
- specify the number of search results displayed on the screen;
- set the maximum number of search results;
- save the search results;
- choose which recordkeeping metadata fields are displayed in search result lists.

7.24 provide relevance ranking of the search results.

7.25 be able to relate an 'extract' of an electronic record to the original record, so that retrieval of one allows retrieval of the other, whilst retaining separate recordkeeping metadata and access controls over the two items.

7.26 allow users who are viewing or working with a record or aggregation, whether as the result of a search or otherwise, to find information about the next-higher level of aggregation of records easily and without leaving or closing the record.

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

Where a graphical user interface (GUI) is employed, the electronic recordkeeping system **must:**

7.27 provide a browsing mechanism that enables graphical, or other display browsing techniques, at any level of aggregation.

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

Rendering: Displaying Records

The electronic recordkeeping system **must:**

7.28 render records that the search request has retrieved.

If the electronic recordkeeping system is storing records in a proprietary application format, it may be acceptable for the rendering to be performed by an application outside the electronic recordkeeping system.

The electronic recordkeeping system **should:**

7.29 render records that the search request has retrieved without loading the associated application software.

This is typically provided by integrating a viewer software package into the electronic recordkeeping system. This is frequently desirable to increase speed of rendering.

7.30 be able to render all the types of electronic records specified by the organisation in a manner that preserves the information in the records (e.g. all the features of visual presentation and layout produced by the generating application package), and which renders all components of an electronic record together.

The organisation must specify the application packages and formats required.

Rendering: Printing

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

The electronic recordkeeping system **must:**

7.31 provide the user with flexible options for printing records and their relevant recordkeeping metadata, including the ability to print a record(s) with recordkeeping metadata specified by the user.

7.32 allow the printing of recordkeeping metadata for an aggregation.

7.33 allow the user to be able to print out a summary list of selected records (e.g. the contents of an aggregation), consisting of a user-specified subset of recordkeeping metadata elements (e.g. Title, Author, Creation date) for each record.

7.34 allow users to print the results list from all searches.

7.35 be able to print all the types of electronic records specified by the organisation. Printing must preserve the layout produced by the generating application package(s) and include all (printable) components of the electronic record.

The organisation must specify the application packages and formats required.

7.36 allow the Administrator to specify that all printouts of records have selected recordkeeping metadata elements appended to them, e.g. title, registration number, date, security category.

7.37 allow Administrators to print the thesaurus.

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

7.39 allow the Administrator to print any and all administrative parameters.

7.40 allow Administrators to print disposal authorities.

7.41 allow Administrators to print the classification scheme.

7.42 allow Administrators to print audit trails.

If the electronic recordkeeping system uses file inventories, it **must:**

7.43 allow Administrators to print the file list (see specification 2.16).

Rendering: Other

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

The electronic recordkeeping system **must:**

7.44 include features for rendering those records that cannot be meaningfully printed to an appropriate output device.

Examples include audio, video, and some websites.

8 > ADMINISTRATION

General Administration

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

The electronic recordkeeping system **must:**

8.1 allow Administrators to retrieve, display and re-configure system parameters and to re-allocate users and functions between user roles.

8.2 provide backup facilities so that records and their recordkeeping metadata can be recreated using a combination of restored backups and audit trails.

8.3 provide recovery and rollback facilities in the case of system failure or update error, and must notify Administrators of the results.

In other words, the electronic recordkeeping system must allow Administrators to 'undo' a series of transactions until a status of assured database integrity is reached. This is only required when error conditions arise.

8.4 monitor available storage space, and notify Administrators when action is needed because available space is at a low level or because it needs other administrative attention.

8.5 allow Administrators to make bulk changes to the classification scheme, ensuring all recordkeeping metadata and audit trail data are handled correctly and completely at all times, in order to make the following kinds of organisational change:

- division of an organisational unit into two;
- combination of two organisational units into one;
- movement or re-naming of an organisational unit;
- division of a whole organisation into two organisations.

When such a change is made, closed files must remain closed, retaining their references to the classification scheme before the change, and open files must either: be closed, retaining their references to the classification scheme before the change, and cross-referenced to a new file in the changed scheme; or: be referenced to the changed scheme, but clearly retaining all prior references to the classification scheme before the change.

Changes to organisational units described above may imply corresponding changes to the classification schemes of the units and their user populations. The term "bulk changes" implies that all aggregations and records affected can be processed with a small number of transactions, rather than needing to be processed individually.

[Note that this element will apply especially where classification schemes are based on an organisation plan.]

8.6 support the movement of users between organisational units.

8.7 allow the definition of user roles, and must allow several users to be associated with each role.

8.8 communicate any errors encountered in saving data to storage media.

Reporting

This section articulates basic reporting requirements. It does not articulate the requirements for a comprehensive reporting sub-system.

The electronic recordkeeping system **must:**

8.9 provide flexible reporting facilities for the Administrator. They must include, at a minimum, the ability to report the following:

- numbers of aggregations, volumes and records;
- transaction statistics for aggregations, volumes and records;
- activity reports for individual users.

8.10 allow Administrators to report on audit trails based on selected:

- aggregations;
- volumes;
- records;
- users;
- time periods.

8.11 be able to produce a report listing aggregations, structured to reflect the classification scheme, for all or part of the classification scheme.

8.12 allow Administrators to request regular periodic reports and one-off reports.

The electronic recordkeeping system **should:**

8.13 allow Administrators to report on audit trails based on selected:

- security categories;
- user groups;
- other recordkeeping metadata.

8.14 include features for sorting and selecting report information.

8.15 include features for totalling and summarising report information.

8.16 allow Administrators to restrict users' access to selected reports.

Altering and Deleting Records

The electronic recordkeeping system **must:**

8.17 include a configurable option to prevent any record, once captured, from being deleted or moved by any Administrator or user. This option should be exercised at the time of configuration.

This requirement does not affect transfer or destruction of records in accordance with a disposal authority.

8.18 allow the Administrator to delete aggregations, volumes and records (subject to the option selected in specification 8.17). In the event of any such deletion the electronic recordkeeping system must:

- record the deletion comprehensively in the audit trail;
- produce an exception report for the Administrator;
- delete the entire contents of an aggregation or volume when it is deleted;
- 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 specification 1.24 – one of which is being deleted);
- inform the Administrator, of any links from another aggregation, or record to an aggregation or volume which is about to be deleted, and request confirmation before completing the deletion;
- maintain complete integrity of the recordkeeping metadata at all times.

This functionality is intended for exceptional circumstances only.

8.19 allow the Administrator to alter the security category of individual records.

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

8.20 allow the Administrator, subject to support for specification 4.39, to alter the security category of all records within an aggregation in one operation. The electronic recordkeeping system must provide a warning if any records are having their security category lowered, and await confirmation before completing the operation.

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

8.21 allow the Administrator, subject to support for specification 4.39, to change the security category of aggregations.

8.22 record full details of any change to security category in the recordkeeping metadata of the record, volume or aggregation affected.

8.23 allow the Administrator to change any user-entered recordkeeping metadata element. Information about any such change must be stored in the audit trail.

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

Redacting Records

The electronic recordkeeping system **must:**

8.24 allow the Administrator to take a copy of a record, for the purposes of redaction.

This copy is referred to as an 'extract' of the record in this specification (see Part A, Section 5, Glossary).

8.25 record the creation of extracts in the record's recordkeeping metadata, including at least date, time, reason for creation and creator.

8.26 store in the audit trail any change made in response to the requirements in this section.

The electronic recordkeeping system **should:**

8.27 provide functionality for redacting (see Part A, Section 5, Glossary) sensitive information from the extract. If the electronic recordkeeping system does not directly provide these facilities, it must allow for other software packages to do so.

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

8.28 prompt the creator of an extract to assign it to an aggregation.

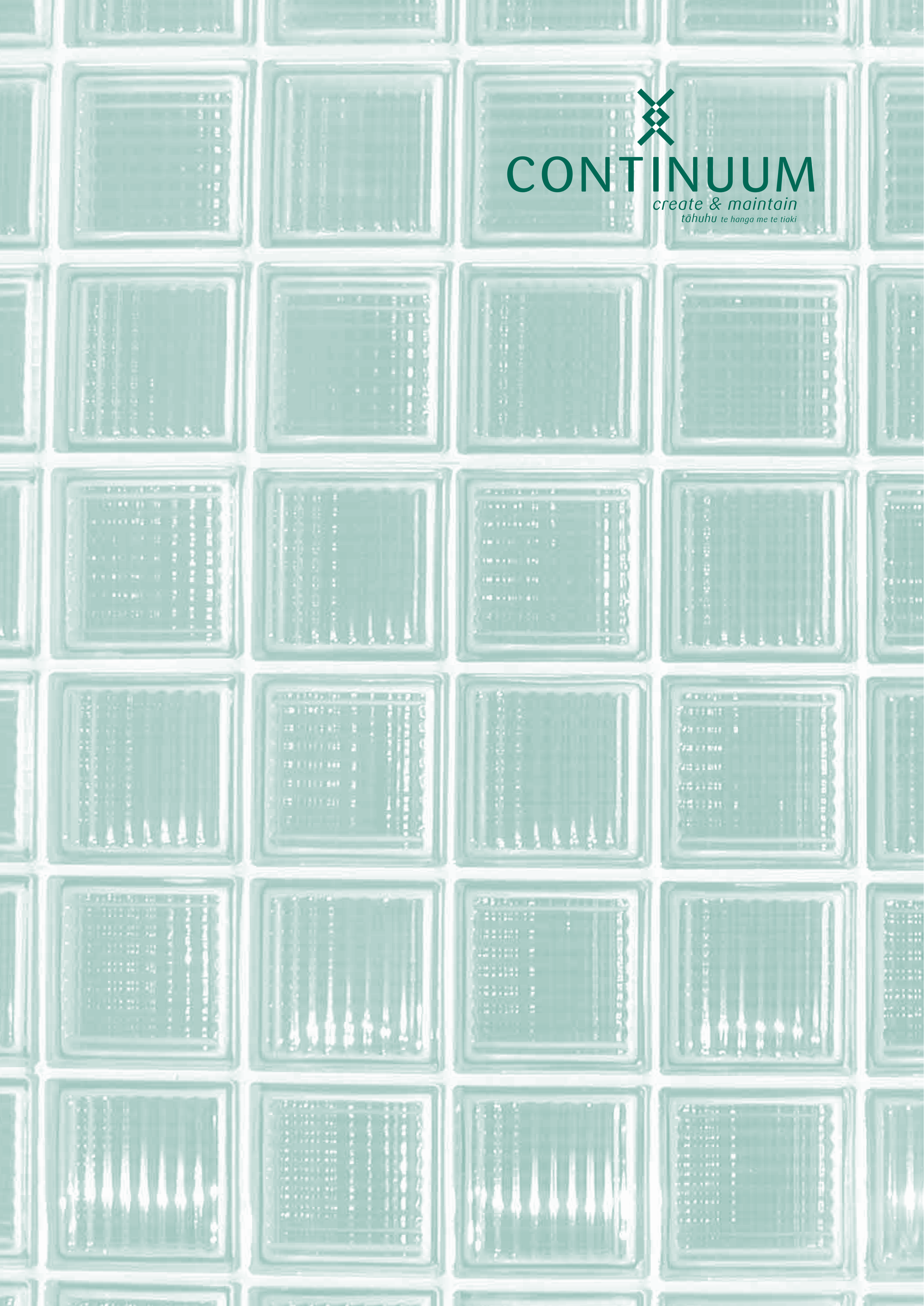
8.29 store a cross-reference to an extract in the same aggregation and volume as the original record, even if that volume is closed.

CONTINUUM

create & maintain

tāhuhu te hanga me te tiaki

NOTES:



CONTINUUM

create & maintain

tāhuhu te hanga me te tiaki

CONTINUUM

create & maintain

tāhuhu te hanga me te tiaki

ISSN 1176-1172

ISBN 0-478-18210-4