



Expression of Interest

Electronic Records Management System

For the purposes of selecting vendors to receive the Request for Proposal we request vendors to complete the following Expression of Interest and return it via email by 12 noon, 26 February 2009.

Responses should be forwarded by email to:

Steve O'Hagan
Knowledge Manager
Crown Law
steve.ohagan@crownlaw.govt.nz

TABLE OF CONTENTS

1.	Introduction.....	2
1.1	Expression of Interest	2
1.2	Closing Details	2
1.3	Submission of Response.....	2
2.	Crown Law.....	2
2.1	Background	2
2.2	Crown Solicitor Network	3
2.3	Current records management practice at Crown Law	3
2.4	Current projects	3
3.	System requirements	3
3.1	An overview of our requirements	3
3.2	Our detailed requirements.....	4
3.3	Usability requirement.....	5
3.4	Current IT Environment.....	5
3.5	User Numbers.....	5
4.	Vendor Requirements	5
4.1	Contact Details	5
4.2	Vendor Details.....	6
4.3	Product or Products or Development Being Offered	6
4.4	Technical.....	7
4.5	Pricing	7
5.	The EOI Process	7
5.1	Completion Instructions	7
5.2	EOI Selection Process.....	8
5.3	Timetable	8
5.4	Terms and Conditions governing this EOI.....	9
5.5	Confidentiality.....	10

SCHEDULE A: CURRENT RECORDS MANAGEMENT PRACTICE AT CROWN LAW

1.	Records management functionality	11
2.	Crown Law records defined	11
2.1	Documentation or evidence of an activity or decision	11
2.2	Created or received by Crown Law	12
2.3	An object held for its usefulness to office as information	12
2.4	Can include both originals and copies of information.....	12
2.5	Variety of media and formats	12
2.6	Digital objects created by office software.....	12
2.7	Digital objects created by specialised business information systems.....	13
3.	How are Crown Law records created?	13
3.1	Core business records	13
3.2	Corporate records.....	13
4.	Location of Crown Law records	13
4.1	Current records.....	13
4.2	Legacy records	15
4.3	Physical records	16
5.	Capture, classification and identification	17
6.	Maintaining records	17
6.1	Retention and disposal of records	17
6.2	Hybrid records.....	18

6.3	Location management	18
6.4	Controls and security	18
6.5	Making records available	19
7.	Weaknesses in current records management system	19
7.1	Inadequate centralisation and integration	19
7.2	Insufficient automation and related poor usability.....	19
8.	Records management roles and responsibilities	20
8.1	Management Board/Practice Manager	20
8.2	Knowledge Services Team.....	20
8.3	Information Technology Manager.....	20
8.4	Technology Trainers	21
8.5	Secretarial/Designated Support Staff are responsible for:	21
8.6	Litigation Support Staff	21
8.7	All staff.....	21

SCHEDULE B – DETAILED RECORDS MANAGEMENT REQUIREMENTS .. 22

1.	Overview	22
2.	Capture	22
2.2	Recordkeeping Metadata	23
2.4	Bulk Capture	27
2.5	Document Types	27
2.6	E-mail.....	28
2.7	Digitisation	28
2.8	Legacy Systems – Electronic.....	29
3.	Classification	29
3.1	Classification Scheme.....	29
3.2	Aggregations (including Volumes).....	30
3.3	Classification Scheme Maintenance.....	32
4.	Identification	32
5.	Maintaining Records	33
6.	Controls and Security	33
6.1	Access.....	33
6.2	Public Access Restrictions	34
6.3	User Access	34
6.4	Audit Trails.....	35
6.5	Backup and Recovery	36
6.6	Tracking Record Movement.....	36
6.7	Authenticity	37
6.8	Data Authenticity	37
6.9	Government Security Classifications.....	37
7.	Retention and Disposal	38
7.1	Destruction Control.....	38
7.2	Disposal Authorities	38
7.3	Disposal Actions.....	39
7.4	Disposal Review Process.....	39
7.5	Metadata.....	41
7.6	Transfer and Destruction	41
8.	Hybrid Record Management	42
8.1	Management of Physical and Electronic Records	42
8.2	Retention and Disposal of Physical and Hybrid records.....	43
8.3	Off-site Storage.....	44
8.4	On-site Storage	44
8.5	Format and Media	44
9.	Client and Archives New Zealand Loan Management.....	44

9.1	General.....	44
9.2	Location Management.....	45
9.3	Audits/Inspections.....	45
10.	Search Retrieve and Render	46
10.1	Searching.....	46
10.2	Retrieving records.....	47
10.3	Displaying.....	47
10.4	Printing.....	48
10.5	Other.....	49
11.	Administration.....	49
11.2	General Administration.....	49
11.2	Reporting	51
11.3	Altering and deleting records.....	52
11.4	Redacting Records.....	53
	Acceptance of Terms and Conditions.....	54

1. INTRODUCTION

1.1 Expression of Interest

The Crown Law Office (Crown Law) wishes to investigate options for an Electronic Records Management System (ERMS).

Crown Law's electronic business systems currently provide some records management functionality for core business records. But there is little integration between systems and some functionality is not provided for well or at all. Solutions are devised within the various teams on an ad hoc basis and are often either manual or have limited accessibility. A primarily manual system is in place to manage corporate records.

Crown Law is seeking Expressions Of Interest (EOI) from vendors that sell and implement electronic records management systems. The purpose of this Expression of Interest is to identify products and implementation partners able to meet a high-level set of criteria relating to Crown Law's requirements. Crown Law intends, at a later date, to issue a Request for Proposal (RFP) to those vendors selected as a result of this process.

1.2 Closing Details

EOI responses **close at 12 noon, 26 February 2009**. Crown Law may extend the closing date for EOI responses at its discretion. All vendor communication in respect of this EOI is to be directed through Steve O'Hagan only.

1.3 Submission of Response

The scope of this EOI is the acquisition and implementation of an ERMS. Other systems outside of an ERMS are not within the scope of this EOI.

Each respondent must submit their response in MS Word using the format that this document is presented in. Responses are to be submitted by email to steve.ohagan@crownlaw.govt.nz

2. CROWN LAW

2.1 Background

Crown Law is a government department whose primary function is to support the two Law Officers of the Crown, the Attorney-General and the Solicitor-General, in the performance of their statutory duties and functions.

Just under half of Crown Law's 210 employees are legal counsel with the rest being support and corporate personnel.

Crown Law's total revenue is approximately \$53m, of which approximately two thirds is received directly from the Crown for provision of agreed outputs, being criminal trial, indictment and appeal services. All other revenue is generated from the billing of their clients being central government departments and Crown agencies.

Although a government department, Crown Law manages its business in the manner of a legal firm. In addition, its reliance on billing revenue and an inability to work within an overdraft requires it to budget, forecast and manage time and dollars to a level not often seen in a government department.

Crown Law is organised into three practice groups, which in turn consist of seven client service legal teams, and a practice management (corporate services) group.

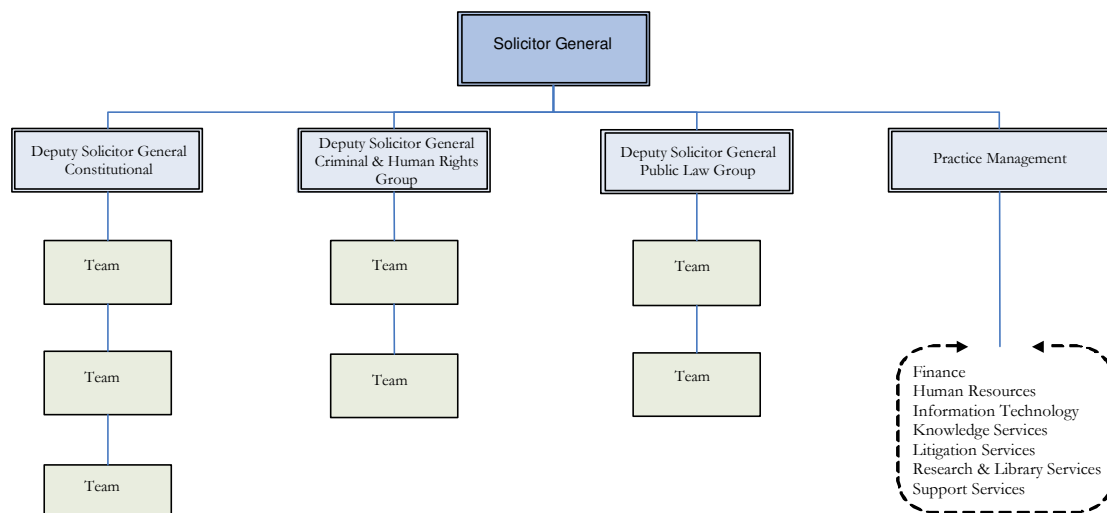


Figure 1 – Crown Law Organisation Chart

2.2 Crown Solicitor Network

Crown Law has responsibility for the supervision and management of the national Crown Solicitor network. There are sixteen Crown Solicitors who are contracted to act on behalf of the Crown in prosecution of criminal cases in their local areas.

2.3 Current records management practice at Crown Law

An outline of current records management practice at Crown Law is set out in **Schedule A**.

2.4 Current projects

Please note we are currently implementing Thomson Elite 3E ([Elite 3E](#)) as our new practice management system to replace Complete Law Office 7 (CLO). So please treat all references in this EOI to CLO as historic. Your ERMS solution must be able to be integrated easily and cost effectively with the Thomson Elite 3E. When considering and discussing functionality and integration into our practice management system, the terms of reference will be Thomson Elite 3E and not CLO.

3. SYSTEM REQUIREMENTS

3.1 An overview of our requirements

Crown Law needs an ERMS that will help it to meet its key duties under the Public Records Act 2005 relating to the creation, maintenance and dissemination of full and accurate records of its affairs. In particular the ERMS must:

- (a) enable capture (including bulk importing) of the content, structure and context of **all** records in order to ensure they are reliable and authentic representations of the business activities or transactions in which they were created or transmitted ¹;
- (b) support and be compatible with Crown Law's classification schemes, and not limit the number of levels in a classification scheme hierarchy or the ability to aggregate records;
- (c) persistently link a unique identifier to every record and associated aggregation;
- (d) automatically include in the metadata of each new aggregation (e.g. folders, volumes) those attributes of its parent aggregation metadata which are common;
- (e) maintain the integrity of a record (including its metadata) once it has been created, (i.e. users should not be able to alter the record or its metadata, but they may be permitted to create a new record by adding to the content, structure or context);
- (f) be able to protect records against intentional or accidental alteration to their content, structure and context throughout their life via access controls, control over alteration of records, audit trails of all recordkeeping actions undertaken by the ERMS, and record location tracking;
- (g) provide a function for specifying disposal authorities, automating reporting and destruction actions, and providing integrated facilities for exporting records and metadata; and restrict the setting up and changing of disposal authorities to authorised persons only;
- (h) be able to capture and maintain metadata relating to non-electronic records as well as electronic records and their associated metadata;
- (i) provide a flexible range of functions that enable a user to search for, retrieve and render records and aggregations, but subject always to access controls so that information intended to be hidden from the user is not revealed;
- (j) include functionality for managing system parameters, backup and restoration, system administration and user administration; for flexible reporting facilities; for the alteration and deleting of records in exceptional circumstances; and for copying records for redaction, and for redaction itself; and
- (k) be capable of allowing the batch upload of data from within the ERMS to Crown Law's Off-Site storage provider's system.

Vendors are asked to comment briefly on their product's ability to satisfy each of these high-level requirements.

3.2 Our detailed requirements

The Public Records Act 2005 includes requirements for public office recordkeeping. These are documented in more detail in various standards issued by the Chief Archivist under section 27 of that Act. The standards include the Create and Maintain Recordkeeping Standard, the

¹ Currently this is understood to consist of 800,000 documents in iManage, at least 1 million emails per year and between 300,000 to 500,000 items in paper form in current and historical manual or physical filing systems.

Electronic Recordkeeping Metadata Standard; the Electronic Recordkeeping Systems Standard; and the Digitisation Standard. The first two are mandatory standards while the other two are discretionary standards.

The current systems and processes at Crown Law don't meet all of the minimum mandatory requirements stipulated in these standards.

Our detailed requirements, as we envisage them at this stage, are set out in Schedule B. While we do not expect vendors to comment at this stage on their product's ability to satisfy each of these detailed requirements, vendors should take the opportunity to make any relevant observations around the practical aspects of implementing the requirements. Any observations made will be taken into account when finalising the detailed requirements for the RFP.

3.3 Usability requirement

In outlining our high-level and more detailed requirements, we expect the ERMS "out of the box":

- (a) to be easily configurable;
- (b) to be intuitive and easy to use;
- (c) to handle the entry, importing and exporting of data, and other functionality, effectively and efficiently, reflecting sound business process; and
- (d) to operate within generally accepted response times.

3.4 Current IT Environment

The proposed system must be capable of running on Microsoft SQL Server.

3.5 User Numbers

There are around 42 core users of the system, being staff in the Knowledge Services and Litigation Support teams, and including 28 secretaries, who initiate the file closing process.

Please describe your user-licensing model.

4. VENDOR REQUIREMENTS

4.1 Contact Details

Name of vendor organisation:	
Physical address:	
Name of individual who responses should be addressed to:	
Phone numbers:	
DDI:	
Mobile:	
Email address:	

4.2 Vendor Details

Please provide the following information:

- (a) A profile of the vendor organisation including, but not limited to, the location and number of staff with experience implementing the proposed solution.
- (b) The number of implementations of the proposed solution that the vendor has completed in the past:
 - (i) 12 months;
 - (ii) 24 months;
 - (iii) 24 months; and
 - (iv) Five years.
- (c) Which organisations they were completed for and the country of residence of the staff that performed the implementation.
- (d) If it is proposed to use another party in supplying any component of software or to undertake any part of the implementation, please provide a profile for each such party; and
- (e) The two most relevant recent implementations of the proposed solution you have completed, including the implementation dates.

4.3 Product or Products or Development Being Offered

Crown Law's requirements have been defined above in Section 3. Please provide the following additional information:

- (a) Name of product being proposed.
- (b) Please list all modules available with this application.
- (c) Briefly define the extent of integration between the modules. Do the modules use a single integrated database?
- (d) Briefly define the extent of web integration and web enablement currently available within the application.
- (e) What release is the version of the application being proposed and when was it released?
- (f) When the application was first released?
- (g) Was the application first developed by your company or by another company? If by another company, who was that company?
- (h) Please list the organisations using this application in New Zealand.
- (i) Please list the organisations using the application in New Zealand with the configuration of modules we expect to employ.
- (j) Please list the organisations using the application elsewhere in the world with the configuration of modules we expect to employ.

- (k) Please describe the process for customising the software for local needs, if required.
- (l) Please describe the process for requesting enhancements to the standard package.
- (m) Please outline the process for managing upgrades when there has been customisation.

4.4 Technical

Please provide the following technical information:

- (a) What development language and toolset has the application been developed with?
- (b) What hardware is required to support the application?
- (c) What database or databases will the application run on?
- (d) What is the architecture that you are likely to recommend?

4.5 Pricing

Crown Law requires some indication of pricing.

All pricing is to be in New Zealand dollars and be exclusive of GST. You must clearly state all assumptions you have made in determining your indicative pricing.

Please answer the following:

- (a) If your pricing structure incorporates a cost for the core application, or a cost per module, with user licence costs in addition to this, please provide the cost of the core application and / or the cost of each individual module?
- (b) What is the cost per user license, please provide price breaks for volume purchases;
- (c) Are your user licences for concurrent or named users?
- (d) What is the average ratio of implementation cost to licence costs?
- (e) What is your hourly charge rate for implementation? (Please detail where there are different costs for different skill sets)
- (f) Will you fix price the cost of implementation?
- (g) What is the annual maintenance cost as a percentage of licence cost?
- (h) Is the annual licence cost payable in the first year?

5. THE EOI PROCESS

5.1 Completion Instructions

- (a) All responses to the EOI must be in the form of a MS Word document using this document as the basis and responding to each section as appropriate within that section.

- (b) Vendors are asked to briefly respond to Crown Law's functional requirements as detailed in Section 3 and to each numbered question / request in Section 4. The EOI response must be provided under each requirement or question / request. Vendors may elect to provide additional information as appendices, but the selection process will focus on the responses in the EOI document. Responses must reflect the features available in the current versions of the solution.
- (c) Please provide a brief management summary highlighting the key characteristics that differentiate your proposed solution.
- (d) A copy of the response is to be signed on behalf of the vendor by a duly authorised officer of the vendor and returned by mail to Crown Law, P O Box 2858, Wellington. This document is expected to arrive within four working days of the EOI response closing date.
- (e) Vendors must acknowledge the acceptance of the terms and conditions of this EOI.
- (f) If vendors have any doubt as to the meaning of any part of this EOI, and this has not been previously clarified, they should document the interpretation that they have used. Any assumption made in the preparation of the response must be briefly documented.
- (g) All contact from the vendor regarding the EOI or subsequent RFP is to be directed to Steve O'Hagan at Crown Law.

5.2 EOI Selection Process

- (a) Crown Law has provided a high level set of requirements and a set of questions relating to the vendor's ability to meet their requirements.
- (b) The responses to the requirements in sections 3 and 4 will be used by Crown Law to determine whether the vendor should be invited to submit a proposal to any future RFP for their recommended solution.
- (c) The issue of and response to this EOI does not create any obligation on Crown Law to enter into any commitment to purchase any particular goods or services. Crown Law reserves the right at all times to decide not to proceed to an RFP.

5.3 Timetable

- (a) The following table shows an indicative timetable for the project.

Activity	Completion Date
EOI released	5 February 2009
EOI responses close	26 February 2009
Selected vendors invited to demonstrate product	12 March 2009
RFP released to selected vendors	21 April 2009
RFP responses close	14 May 2009
RFP evaluation and vendor short list completed	28 May 2009
Preferred vendor selected	4 June 2009

- (b) Crown Law reserves the right to vary this timetable, at any time, without notice.

5.4 Terms and Conditions governing this EOI

- (a) Crown Law shall have no liability for any consequences whatsoever arising in any way from reliance on information it provides, or for any cost or loss to any vendor:
 - (i) if a vendor is not invited to submit a future proposal; or
 - (ii) if this EOI is cancelled, suspended or varied; or
 - (iii) if Crown Law exercises any of its rights under this clause; or
 - (iv) for any failure to notify a potential vendor of any variation or change to this EOI.
- (b) Crown Law reserves the right to liaise or negotiate without restriction with any vendor or any other person at any time on any matter contained in a response, without disclosing this to, or involving any other vendor or person.
- (c) Nothing contained or implied in this EOI shall oblige Crown Law to discuss, justify or give reasons for any of its decisions or actions relating to or arising from this EOI or any response.
- (d) There is no obligation on Crown Law to accept for further consideration any response to this EOI. Crown Law reserves the right to accept for further consideration responses which are not the lowest in price or which do not offer the highest service levels.
- (e) This EOI process does not create any contractual relationship between Crown Law and any respondent to this EOI in respect of the supply of solutions or services sought under this EOI.
- (f) In submitting a response to this EOI, the vendor is deemed to have accepted the terms and conditions stated in this EOI.
- (g) Each vendor shall examine and be deemed to have examined, the EOI and any other information supplied by Crown Law in writing and shall satisfy itself and be deemed to have satisfied itself as far as practical before responding as to the correctness and sufficiency of the response.
- (h) At any time Crown Law reserves the right to:
 - (i) cancel or suspend this EOI; or
 - (ii) vary the terms of this EOI, including varying any policy or criteria relating to the evaluation of responses; or
 - (iii) vary any date, timing or processes referred to in this EOI.
- (i) Crown Law, may insert addenda to the EOI prior to the closing of submissions (or prior to any extension which Crown Law may nominate in its absolute discretion) for the purposes of clarifying this EOI.
- (j) The vendor must acknowledge receipt of all addenda with its submission. All addenda issued will become part of the EOI.
- (k) Crown Law will not be responsible for, or pay any expense incurred by a supplier in the preparation of their proposal or the evaluation of it.

- (l) Crown Law has made every endeavour to provide information relevant to the requirements that is as accurate as possible. Some of this information may not be completely up-to-date. Where the accuracy of information provided by Crown Law is considered by the vendor to be materially relevant to the response being submitted, then the vendor must indicate this in the response.

5.5 Confidentiality

- (a) All documents received by Crown Law will be kept confidential, except as required by law, including the Official Information Act 1982.
- (b) All submitted responses become the property of Crown Law and will not be returned to vendors.
- (c) No supplier shall, at any time, make any public statement in relation to this EOI without prior written consent from Crown Law.

All vendors are required to acknowledge in their proposals that they accept the terms and conditions set forth in sections 5.4 and 5.5. Crown Law may reject proposals that fail to give such acknowledgement.

SCHEDULE A – CURRENT RECORDS MANAGEMENT PRACTICE AT CROWN LAW

1. RECORDS MANAGEMENT FUNCTIONALITY

Crown Law's electronic business systems currently provide some records management functionality. This functionality is outlined below.

The diagram in Figure 2 below is an illustration of general Records Management functionality in relation to current systems at Crown Law. The electronic document management system and electronic records management system have been grouped together in this model to reflect their overlapping records management functionality. Worksite is represented separately as in this context it is primarily a tool for disseminating and accessing information.

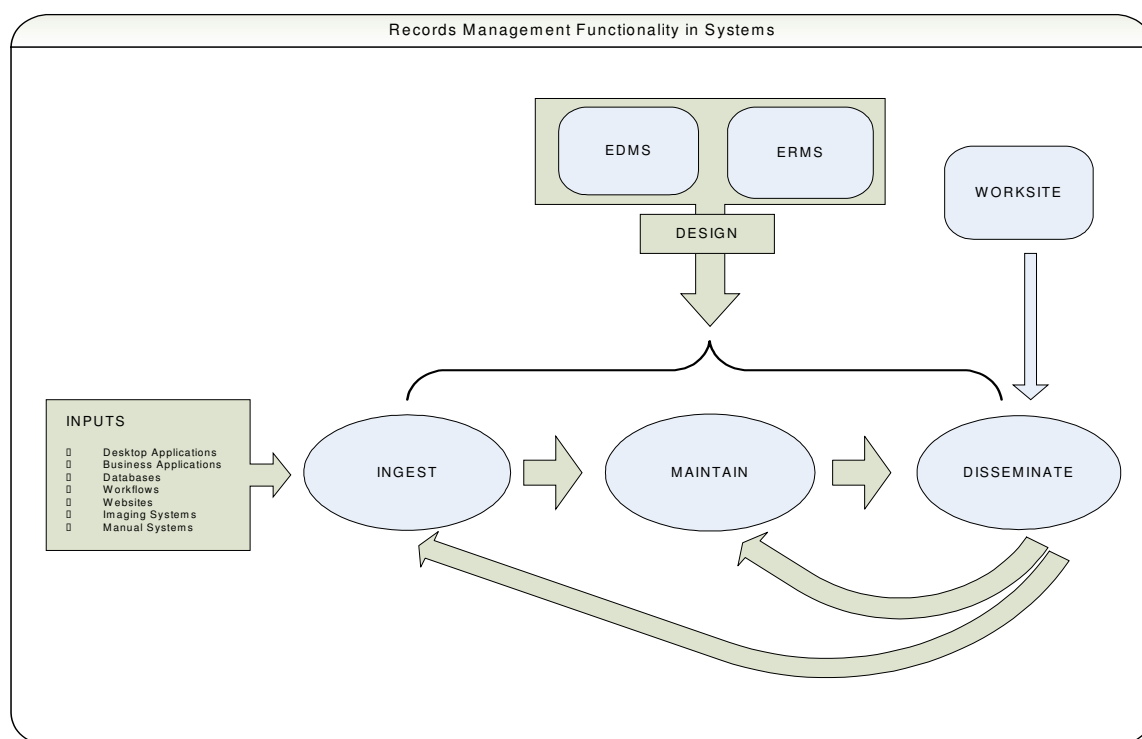


Figure 2 – Model of Records Management Functionality

2. CROWN LAW RECORDS DEFINED

The following descriptions summarise what a record is in the Crown Law context.

2.1 Documentation or evidence of an activity or decision

Examples:

- Advice
- Bill payment/invoicing
- Litigation Management Plan
- Minutes

- Contracts
- Correspondence
- Court documents
- File status/file closing process
- Payroll
- Peer Review Form
- Report to Attorney-General
- Tenders

2.2 Created or received by Crown Law

Examples:

- Client matter records
- Inwards correspondence (electronic or physical)
- Invoices
- Pleadings or documents filed by opposing counsel

2.3 An object held for its usefulness to office as information

Examples:

- Casebooks
- Court contact details
- Client details
- Research

2.4 Can include both originals and copies of information

Examples:

- Hard copy opinion books and scanned opinions
- Research documents
- Scanned client or Archives NZ documents

2.5 Variety of media and formats

Examples:

- Paper
- Electronic
- Letters
- Sound recordings
- Emails
- Web pages
- Digital images
- Maps & plans
- CDs, DVDs, cassette & video tapes
- Photographs, negatives, film
- Microforms
-

2.6 Digital objects created by office software

Examples:

- Documents (MS Word, PDF etc)
- Digitised or scanned images

- Emails
- Presentations (MS PowerPoint etc)
- Simple databases (MS Access etc)
- Spreadsheets (MS Excel)
- Still and moving images

2.7 Digital objects created by specialised business information systems

Examples:

- Client record, Matter record, Draft bills, Fee earner record etc (Financial/Practice Management System)
- Workspace pages & content
- Staff records, leave records, payroll (PS 2000)
- Scanned images, Discovery lists etc (Signature Cannae)

3. HOW ARE CROWN LAW RECORDS CREATED?

Crown Law Office records are created and received in the course of either performing our core business functions or of managing the office and its infrastructure.

3.1 Core business records

Crown Law's core business is to provide legal advice and representation to the Crown; undertake Law Officer functions; assist with the conduct of criminal appeals; supervise the Crown Solicitors in their prosecution functions; and provide advice on the establishment and development of legal service provision within government departments and agencies. The records resulting from these activities are predominantly held as part of the "Client/Matter" filing system.

This system comprises physical files managed through the Practice Management System (currently Complete Legal Office) and electronic records managed through iManage/DeskSite 8.2 and Worksite.

3.2 Corporate records

The records created as a result of management of the office itself are primarily held in the "Corporate Filing system". These include financial, human resource, information management, strategic planning and policy, and general administrative records. This system comprises a classification structure defined in an Excel spreadsheet and corresponding physical files and electronic documents managed through iManage/DeskSite 8.2. There is currently little correlation between electronic and physical corporate records.

Some Crown Law Office records, including the client matter and advice files, require specific management because the organisation operates in part as a professional legal services agency.

4. LOCATION OF CROWN LAW RECORDS

4.1 Current records

Records are created in or captured into a number of current business and records management systems at Crown Law. These include both electronic and manual systems and

systems that operate as a combination of the two. Records are also created in a variety of ad hoc systems operating in various teams throughout the office.

The diagrams in Figure 3 below show the current systems with descriptions of the types of records created in, or captured into, each of them. Capture and creation relationships between systems are also indicated in the diagrams.

Open physical records are stored in team storage areas and centrally in the Corporate Services storage area. Closed physical records are stored centrally in the Records storage area and off-site in the Online Security Services Limited commercial storage facility.

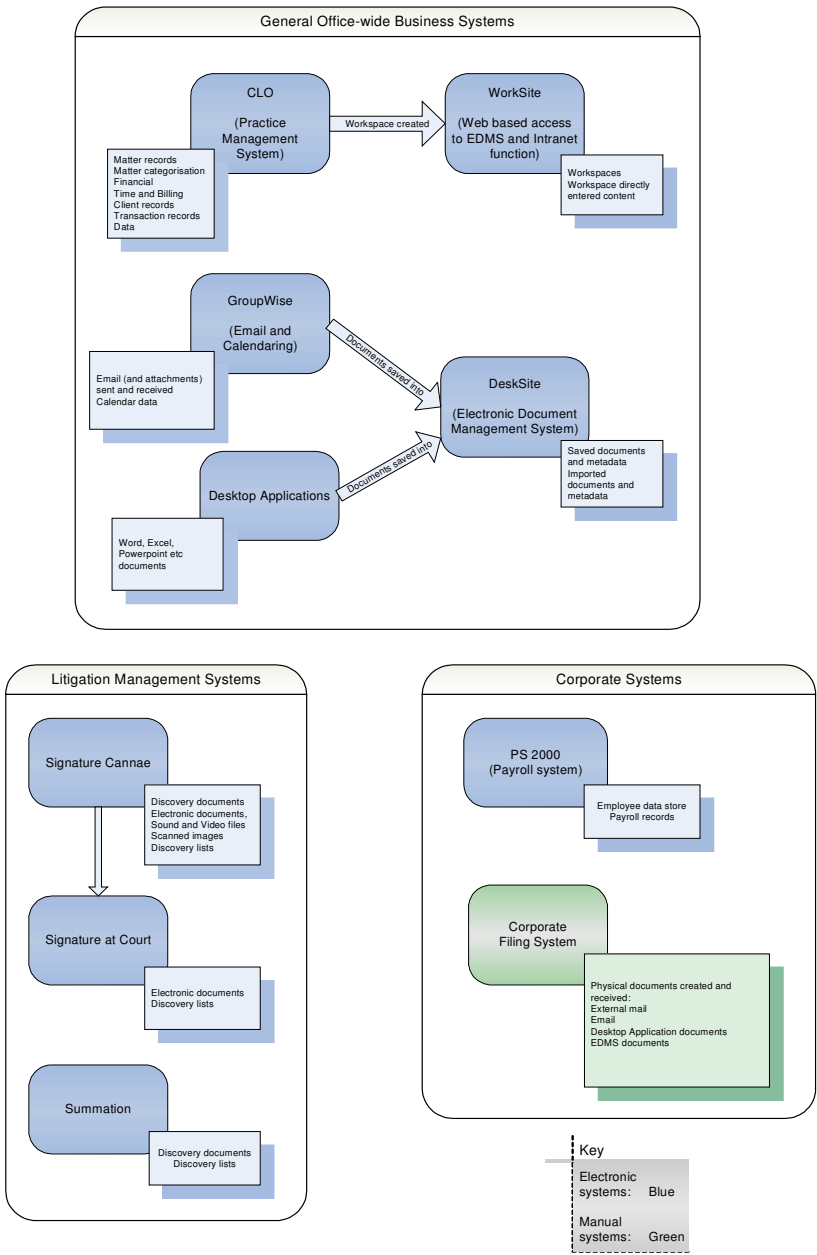


Figure 3 – Business systems in which records are created and stored

4.2 Legacy records

Closed records are also stored in a number of superseded systems. These include one electronic system (Exsys/Soft Solutions) and various manual systems. Figure 4 below illustrates the various legacy systems with descriptions of the records held in them.

Physical legacy records are stored on-site centrally in the Corporate and Records storage areas and off-site at the Online Security Services Limited commercial storage facility.

A small number of closed records have also been transferred as archives to Archives New Zealand.

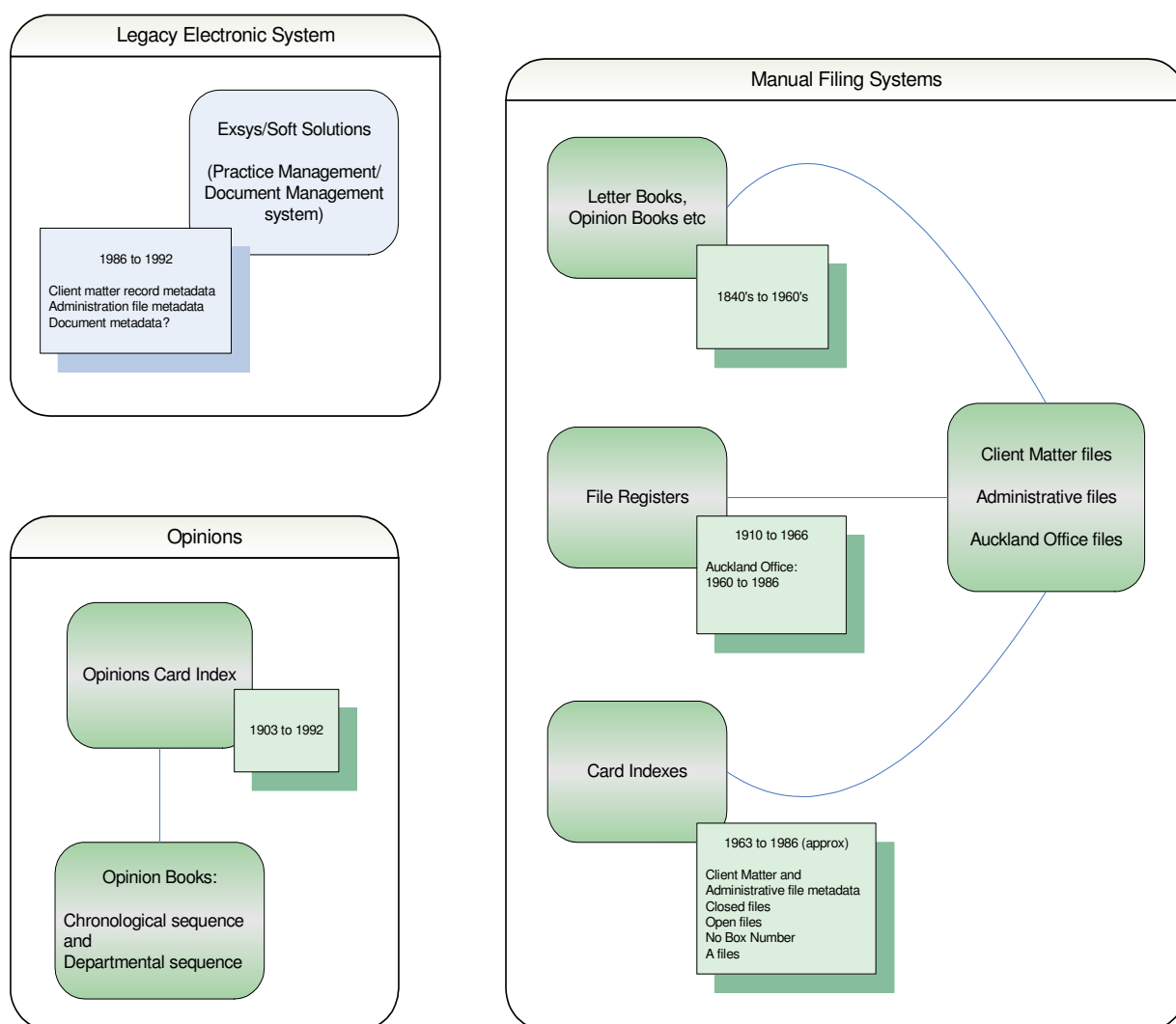


Figure 4 – Legacy Systems in which records are stored

4.3 Physical records

Physical records are captured into the current business systems outlined in Figure 3 above. The diagram in Figure 5 below illustrates the range of record classes these physical records consist of and are captured as.

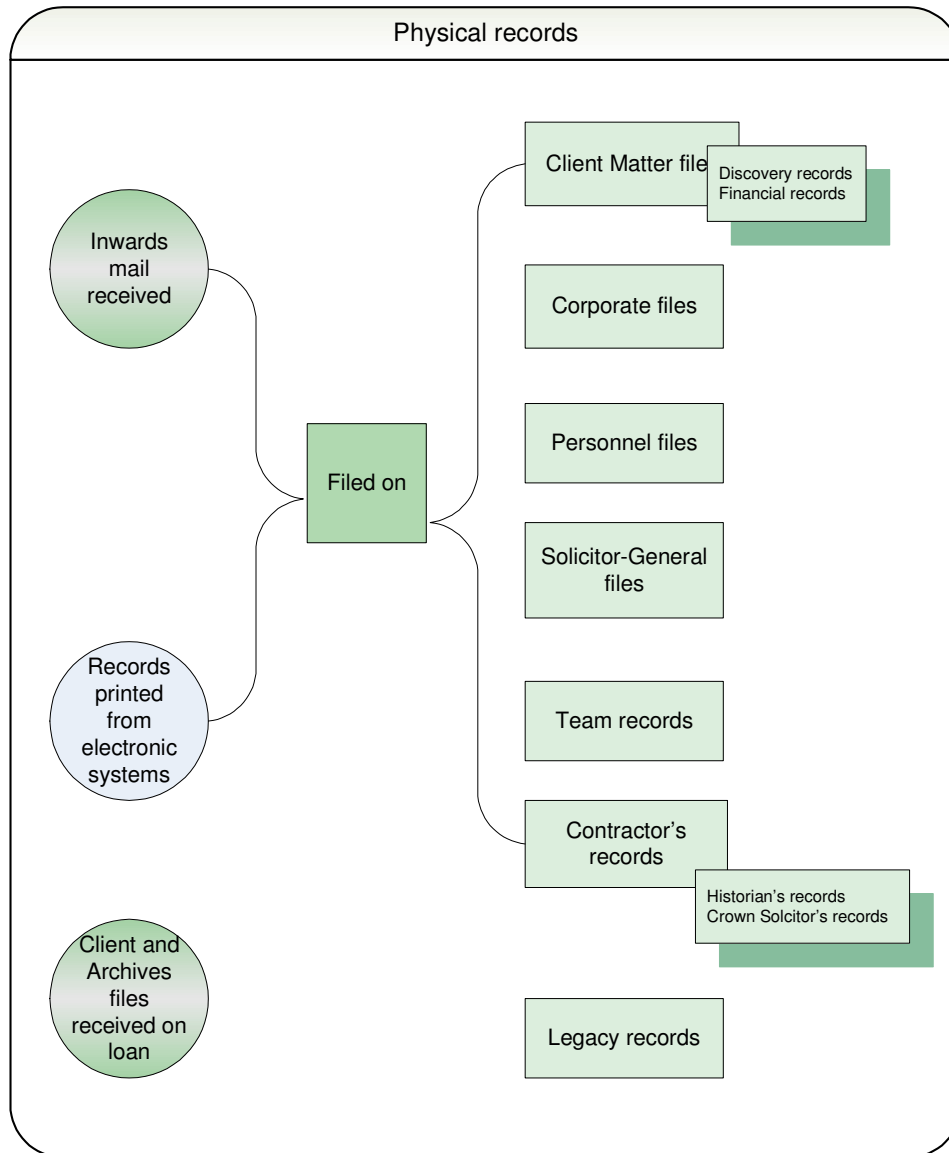


Figure 5 - Records system holding physical records

5. CAPTURE, CLASSIFICATION AND IDENTIFICATION

The current practise management system, CLO, supports the classification of client matter files through the definition and generation of Client and Matter reference codes and the collection of work group and work type codes as part of matter record metadata.

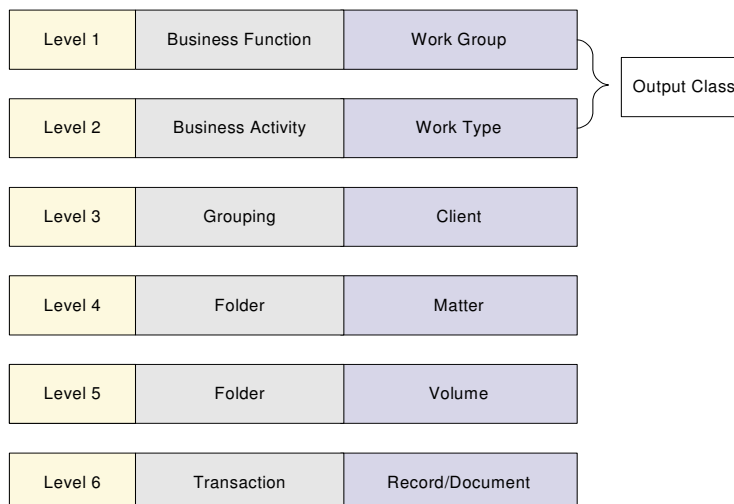


Figure 6 – Functional classification model in Crown Law environment

Matter record metadata captured in CLO also includes the record title, date opened, date closed, file status, location management information. Other records management metadata such as tracking information is sometimes recorded informally in notes fields within CLO.

Records are captured into, and have identification and some classification applied in the Electronic Document Management System (iManage/DeskSite 8.2). Records are also created in Worksite (the web version of iManage).

6. MAINTAINING RECORDS

The Client Matter reference defined through CLO provides the hybrid record link between physical and electronic components of a matter record.

Location Management and off-site storage management data is held in CLO including in the “File No” field (off-site storage box number) and bar code information in “AR Notes” field.

User access profiles are established for iManage/DeskSite 8.2, CLO and Worksite.

Audit trail information is collected as the history of documents in iManage/DeskSite 8.2.

6.1 Retention and disposal of records

The retention and disposal function uses the capture, classification and identification information to document all records and records classes created by Crown Law. The value of each record class or record is then determined using a process of appraisal.

The result of the appraisal examination is a set of recommended disposal actions for each class of record. These will generally define a period to be retained at Crown Law, a period to be

retained in storage and whether the record should ultimately be destroyed or retained as an archive (at Archives New Zealand). In the electronic environment disposal categories are often defined in systems at the beginning of the record's life or before it has been created.

Disposal recommendations approved by the Chief Archivist, Archives New Zealand result in Disposal Authorities, which together form an office-wide, Retention and Disposal Schedule.

Once approved disposal authorities have been obtained, the implementation involves reviewing disposal candidates against the Crown Law Retention and Disposal schedule and confirming authorisation for disposal actions; managing transfer, migration or destruction of records or record groupings; and establishing or confirming appropriate public access restrictions on any records transferred to Archives New Zealand as archives. Confirmation of disposal can involve both Records staff and Senior Managers in the area responsible for the original creation or use of the records.

6.2 Hybrid records

Management of hybrid records (those with both physical and electronic components) includes ensuring that they have the same classification, that the open and close dates of physical and electronic volumes are synchronised, that they are accessible as an entity and that the disposal process is applied to both.

6.3 Location management

Location control is a records management function that is essential to ensure the maintenance of access to information for users and the safety of Crown Law records. It requires all storage types, storage locations, and all home locations for physical records of any format or media to be defined. Systems should be in place to then record any location movements. The resulting tracking record enables all users to identify the location of records at all times.

Location management systems often include a "Request" system. This is used when user access to some or all storage areas is limited or where staff in particular roles provide this service to other staff, for example: Secretaries providing a retrieval service for their assigned Counsel. Access to records in these cases is provided through an issuing system. Records stored off-site are also accessed using a request system, both internal to enable staff to order records and external to enable them to be retrieved from the off-site storage provider's facility.

Storage type and location information is also used by Records staff to manage records of non-standard format or media; and records requiring additional physical security; and to allocate storage space to particular teams or users.

Crown Law regularly receives records belonging to or held by Clients and Archives New Zealand. These records need to be managed through a loan management system and require similar location management as Crown Law records to ensure their safety and accessibility while they are at Crown Law.

6.4 Controls and security

Current controls are done through the doc management system Read Access, Read/Write, Full Access & no Access

In regards to files, all secretaries have the ability to recall files, if they know the matter number, they have the access to see what file's there are if they are offsite. In regards to "live" files, records staff has no control over who can or cannot see them.

6.5 Making records available

Records management functions include facilitating user access to information according to defined authorities. This is achieved through searching, retrieval and reporting systems and services. These systems have to enable users to identify the records and record classes that contain the information they need to undertake their roles.

After receipt of request for a file, records staff take the following action:

- (a) Search CLO for matter number;
- (b) Obtain item barcode number from information held in AR-Archive Matters Notes field in CLO
- (c) Either locate item on-site or place request for item with Crown Law's off-site storage provider.

7. WEAKNESSES IN CURRENT RECORDS MANAGEMENT SYSTEM

7.1 Inadequate centralisation and integration

Records Management functionality is provided through a variety of electronic and manual systems at Crown Law. There is currently little integration between systems and some functionality is not provided for well or at all. Solutions are devised within the various teams on an ad hoc basis and are often either manual or have limited accessibility. This results in unmanaged record creation and maintenance and a lack of continuity throughout the office. The likelihood of associated risks occurring, including that information required for business purposes is lost and that Crown Law is unable to account for its actions and decisions, is increased.

Increasing the integration of systems and establishing of office-wide systems covering all records management business needs provides an opportunity for increasing efficiency in business operations. This would be achieved through the significant reduction in duplication of work effort, increased accessibility of information required by staff to do their jobs, and reducing the time required to undertake records management activities and functions.

7.2 Insufficient automation and related poor usability

The Practice Management System, currently CLO, provides basic matter level records management for core business records. A primarily manual system is in place to manage corporate records.

A lack of awareness of and reluctance to use manual systems, together with the staff need to allocate their time, has lead to CLO being used to manage administrative records in preference to the Corporate Filing System. CLO also offers users advantages of an electronic system such as searching and basic location management facilities.

The policy statements included in the Management Board approved Crown Law Recordkeeping Policy support improvements to systems managing records.

8. RECORDS MANAGEMENT ROLES AND RESPONSIBILITIES

8.1 Management Board/Practice Manager

The Management Board/Practice Manager is responsible for:

- (d) Authorising the purchase of an Electronic Records Management system or any other software or system components identified as required to enable essential records management functionality to be provided.
- (e) Providing sufficient resourcing to configure and implement any system, software or tool purchased.
- (f) Supporting the implementation and use of the system.

8.2 Knowledge Services Team

The **Knowledge Services Team** is responsible for:

- (a) Identifying business requirements for an Electronic Records Management system and providing these to the Information Technology Manager.
- (b) Obtaining management agreement with the Electronic Records Management System Business Requirements.
- (c) Making recommendations to the Management Board on ERMS system requirements.
- (d) In conjunction with Business System owners, identifying configuration requirements for any Electronic Records Management system purchased.
- (e) Defining records functionality configuration requirements and associated business rules for any system purchased.
- (f) Assisting with the implementation and supporting use of any ERMS system purchased.
- (g) Undertaking system maintenance and operational tasks defined as central Records tasks.
- (h) Maintaining an overview of records systems to ensure that the structures are working effectively and that they support organisational and public accountability.

8.3 Information Technology Manager

The **Information Technology Manager** is responsible for:

- (a) Identifying how the Electronic Records Management system Business Requirements can be met and reporting this to the Knowledge Manager.
- (b) Undertaking configuration of software/systems according to requirements defined by the Knowledge Services team.
- (c) Maintaining the system and providing technical knowledge in support of it.

8.4 Technology Trainers

The **Technology Trainers** are responsible for:

- (a) Ensuring that all staff receive appropriate training in the use of the system.
- (b) Reporting any issues identified while undertaking training to the Knowledge Manager or Records Coordinator.
- (c) Secretarial/Designated Support Staff

8.5 Secretarial/Designated Support Staff are responsible for:

- (a) Undertaking system maintenance tasks assigned including the creation and closing of volumes, assigning home locations, printing file labels etc.
- (b) Utilising location management and request functionality provided.

8.6 Litigation Support Staff

Litigation Support staff are responsible for:

- (a) Utilising the features provided for the management of client and Archives New Zealand records on loan including capturing loan record descriptions into the system and using tracking functionality.

8.7 All staff

All staff are responsible for:

- (a) Creating records.
- (b) Capturing records into appropriate systems with required metadata.
- (c) Updating location information for any record they retrieve or re-locate.
- (d) Following business rules defined in relation to any Electronic records
- (e) Management system implemented.

SCHEDULE B – DETAILED RECORDS MANAGEMENT REQUIREMENTS

1. OVERVIEW

The detailed Electronic Records Management System requirements are arranged in sections corresponding to the model illustrated in the diagram below (figure 6).

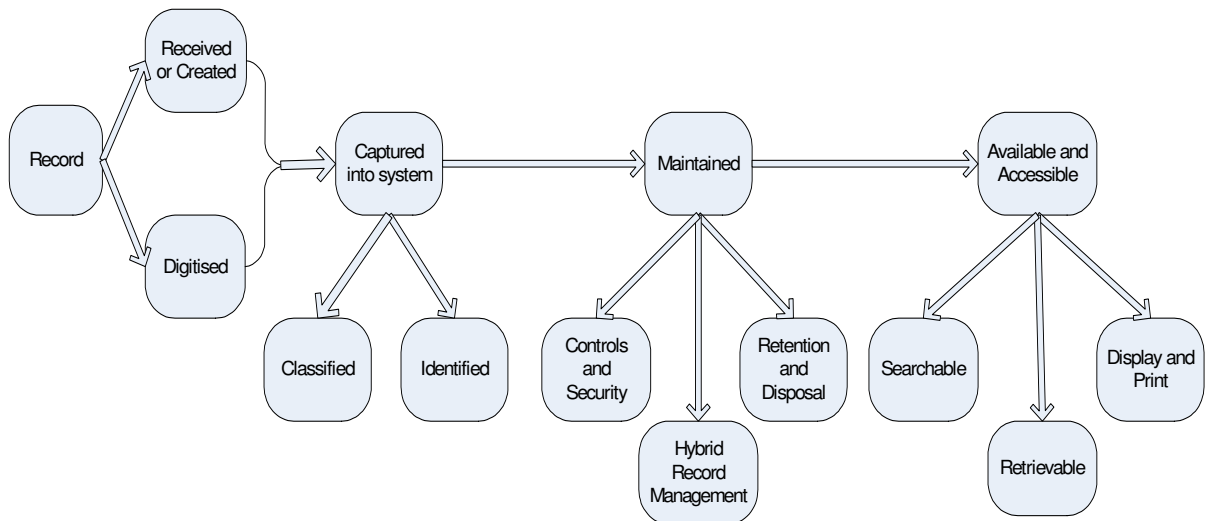


Figure 6 – Detailed requirements model

2. CAPTURE

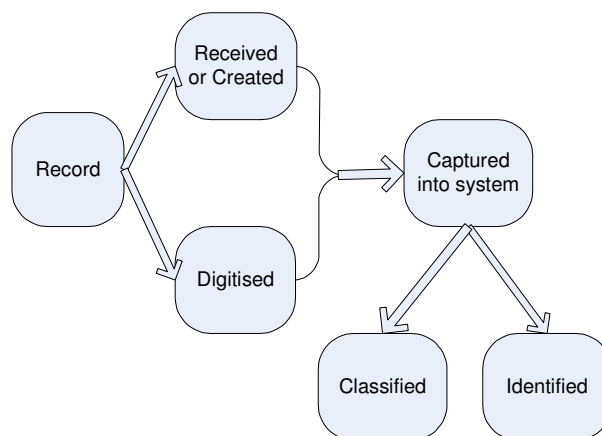


Figure 7 – Capture process

2.1 Capture Processes

- (a) Integrate with business applications, including the Practice Management system (CLO), Litigation Management systems (Signature Cannae and Summation) and the Payroll system (PS 2000), so that records created by them can be captured within the electronic records management system in their original file formats.
- (b) Indicate when an individual record is captured within the electronic records management system.
- (c) Prevent the alteration of the content of any record by any user or administrator once it has been captured into the system and has been certified as the final version.
- (d) Allow capture of individual records directly into the Electronic Records Management System.
- (e) Support the management of records created by firms and individuals employed to undertake work for Crown Law on contract through the ability to capture these records.
- (f) Allow a user to pass electronic records to another user to complete the capture process. For example, to add additional metadata.
- (g) 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 records management system must allow this name to be changed at the time of capture into the electronic records management system.

2.2 Recordkeeping Metadata

- (a) Allow metadata elements to be captured for each record and ensure they are linked to the record over time. These must include the date and time of capture of each record.
- (b) Allow the Records Administrator to define and redefine the records management metadata elements associated with each record, including whether each element is mandatory or optional.
- (c) Allow metadata to be automatically extracted from the software application in which the record was created; from the operating system; or from the electronic records management system. Allow users to enter additional records management metadata during record capture or at any later stage of processing.
- (d) To support the following metadata elements:

Point of Capture Metadata:

Field	Field Type
Unique Identification Number	Unique Number
Client Name	Text
Client Code	Text
Matter name	Text

Field	Field Type
Matter Code	Number
Record Type	List (Text)
Item Description/Title	Text
Record Status	List (Text)
Open Date	Date (dd/mm/yyyy) and time
Close Date	Date (dd/mm/yyyy) and time
Volume Number (Part in Doc Project)	Number
Volume Created By	Text
Notes	Text
Security Classification (Government)	List

Record-keeping Metadata:

Field	Field Type
Vital Records Indicator	Yes/No
Thesaurus Term	Text (Keywords)
Record Number	Number/Text (or any mixed format)
Matter Cross Reference	Text (Alpha/Numeric Code or any mixed format)
Alternative Number	Number/Text (or any mixed format)
Archives NZ Identification Codes	Text/Numbers (various formats)
Client File Number	Text/Numbers (various formats)

Location Management Metadata (required for physical files only):

Field	Field Type
Bar Code Number	Variable
Box Number	Number/Text
Media	List
Format (Record Type in Doc Project)	List
Home Location Code/Description	Text/Bar code
Current Location Code/Description	Text/Bar code
Location History	Audit Trail
Location Type	List
Archives NZ Identification Codes	Text/Numbers (various formats)
Client File Number	Text/Numbers (various formats)

Retention and Disposal Metadata:

Field	Field Type
Appraisal Decision	List
Disposal Authority Number	Number

Field	Field Type
Disposal Authority Name	Text
Disposal Decision Number	Number
Retention Period On-Site	Period of time/number
Retention Period Off-Site	Period of time/number
Disposal Action	List
Public Access Restriction	List
Privileged Access Authority	Number/Text

Digitisation:

Field	Field Type
Digital Image Identifier	Unique number
Date and Time of Digitisation	dd/mm/yyyy and time
Name of Agent Associated with Digitisation Process	Text
Capture Device	List
System Maintenance Information	text

- (e) Ensure that the values for records management metadata elements conform to specified formats defined when the system is configured.
- (f) Record the date of opening of a new folder (at any level including volume) within the records management metadata associated with it.
- (g) Automatically include in the records management metadata of each new folder (at any level including volume) metadata that is associated with its position in the folder structure/classification scheme. For example, each volume of a matter should inherit the Client Name, Matter title, matter code etc as part of its metadata.
- (h) Ensure that the original version of metadata is retained as a viewable history record when changes to metadata are made.
- (i) Ability to re-use previously entered data in the next entry operation (defaulting to previously entered data) to reduce the amount of keystrokes required to undertake multiple entry.
- (j) Ensure that any “tab” level title information in WorkSite is included in the folder metadata, as metadata can’t be assigned at the tab level.
- (k) Allow generous field sizes for titles and descriptions of records or folders (at any level including volumes) to prevent the need for abbreviation of this information.
- (l) Allow flexible pick-lists to be set up for users on specified fields, so that they can select options from lists customised according to their role or team (e.g. for location codes, etc)

For example:

Location codes:	Enable pick lists of codes to be limited or prioritised to display those most used by a particular team, by the Counsel a particular Secretary is responsible for, or for a particular purpose such as client file storage etc. as the only or first options.
Corporate Filing system:	Enable parts of the file plan most likely to be used by users in particular roles to be displayed as the first (or only) options for selection.

- (m) When a record object is captured the following recordkeeping metadata must be collected: a unique identifier; a title; date of creation; who created the record; what business is being carried out and the business application the record was created in.
- (n) Ensure that Business application activities/operations don't prevent the capture and maintenance of accurate records management metadata. For example: Ensure that closure of the financial time recording facility for month and year end activities doesn't impact on the capture of accurate open dates for new matters created.
- (o) Ensure that previous matter status metadata is retained when any changes are made to the status of a matter and ensure it is accessible as a field history record on an ongoing basis.
- (p) Record each closing/re-opening action separately and maintain a full record of each of these actions and the history of them (date, what, who, why).

2.3 Aggregation/Volumes

- (a) Ensure that all records captured within the electronic records management system are associated with at least one folder within the classification scheme.
- (b) No limit should be placed on the number of records that can be captured in a folder (at any level of the classification), or on the number of records which can be stored in the electronic records management system, unless it is required to maintain parity between electronic and paper volumes.
- (c) Ensure that following a pointer or reference to a record, whichever folder or folder level that pointer is located in, will always result in correct retrieval of the record and that if a record location changes any pointers that reference that record are re-directed.
- (d) Where an electronic object has more than one version, allow users to choose one or more of the following options:
 - (i) register all versions of the object as one record;
 - (ii) register one version of the object as a record;
 - (iii) register each version of the object as a record.
- (e) The system should enable records to be assigned to multiple folders (at any level) without them being duplicated.
- (f) Issue a warning if a user attempts to capture a record that has already been captured in the same folder (at any level).

2.4 Bulk Capture

- (a) The electronic records management system must be able to accept bulk capture of records from, for example, an electronic document management system, a workflow application, or records exported from other records management and document management systems.
- (b) Electronic records captured in bulk should be able to be captured in their existing format, with relationships between the components of individual records retained and without the content or structure of the records being altered.
- (c) Metadata associated with the records involved should be retained along with the correct relationship between individual records and their metadata.
- (d) The folder/classification structure that the records belong to, metadata associated with it, and the relationship between records and this structure, should be able to be retained.
- (e) For example, if a set of Client Matter records were being captured in bulk, the relationship between each matter record and the relevant client record should be retained; and the relationships of records as client records (as a folder level) or matter records (as a folder level) or matter records as all relating to one client record should be retained.
- (f) It should be possible to apply additional metadata to all of the records involved in a bulk capture operation to record the system they were captured from.
- (g) Audit trail information directly associated with the record and/or folder (at any level) should be imported and securely retained.

2.5 Document Types

- (a) Enable records created in standard office application file formats (MS Word, Excel, PowerPoint, MS Access etc); in the e-mail client (GroupWise), in imaging applications (e.g. Signature Cannae); and in web authoring tools (Worksite) to be captured into the electronic records management system.
- (b) Be able to extend the range of file formats supported as new file formats are introduced.
- (c) Allow users to capture and store records in their native format.
- (d) Capture electronic records made up of more than one component so that the relationship between the components and the structural integrity of them is retained.
- (e) Allow easy capture of records made up of more than one component, preferably with one action such as single click.
- (f) Enable records made up of more than one component to be managed as a single unit.

2.6 E-mail

- (a) Allow users to capture e-mails (text and attachments) as single records from within the email client.
- (b) Provide users with the options to capture emails that have attachments as the e-mail message only, the e-mail message with the attachment(s), or the attachment(s) only.
- (c) Ensure that e-mail transmission data is captured as part of the records management metadata and linked to the email on an ongoing basis.
- (d) Ensure that a human-readable version of an e-mail message address is also captured if it exists. For example, for “Joe Bloggs” <joe.bloggs@ crownlaw.govt.nz>, “Joe Bloggs” is the human-readable version of the e-mail address joebloggs@crownlaw.govt.nz.

2.7 Digitisation

- (a) A confirmation process should be included to support quality checking of digitised images before they are accepted into a business process as a master copy.
- (b) Ensure that digitised records are unalterable in all storage media and that master copies are retained in secure storage.
- (c) Ensure that digitised records are (re) producible in their original format on request.
- (d) Provide a facility to document any use of techniques that enhance the digitised image to make the image have a more exact resemblance to the original, or reproduce the source record’s appearance more faithfully, during the digitisation process.
- (e) If annotations are added to images after capture, they should be managed as overlays that do not change the actual image and it should be possible to print the image with or without the annotations.
- (f) Ensure that images can be displayed in a form and quality that enables associated business processes to be carried out.
- (g) Support the establishment of links between associated documents that are to be regarded as a single item, so that the digitised image can accurately represent the source record.
- (h) The digital image and the source record should be linked.
- (i) Enable the metadata controlling the relevant business process, and the records management functions associated with the business process, to be inherited by the specific digital image.
- (j) The system must support the management of the digital output of digitisation, whether digitisation is part of an ongoing business process or carried out as a retrospective project.
- (k) All digitised images must be assigned metadata to document digitising processes and to support ongoing business processes.

- (l) Metadata specific to the particular image and the imaging process; and metadata about the record, the business being transacted and the agents associated with the business must be captured.
- (m) In addition to inherited metadata, the following metadata must be captured: unique digital image identifier, date and time of digitisation, the name of the agent associated with the digitisation process, capture device, and if possible system maintenance information.
- (n) In business-process related digitisation, records metadata must be incorporated into the electronic records management framework and be consistent with ISO 23081. Where the digital image is to be used as a record in current or continuing business, the system managing the business process that will use the image, for example Signature Cannae, should be integrated with records control systems.
- (o) Scanner operations should be integrated with the Electronic records Management system to streamline capture.

2.8 Legacy Systems – Electronic

- (a) Support record and item description data held in legacy electronic records management systems (e.g. Exsys/Soft Solutions) being accessed and managed in an integrated way along with data in current systems.
- (b) The integrity and authenticity of the original information in legacy systems must be maintained throughout any migration process undertaken and once it is being managed through an electronic records management system.
- (c) Bulk importing of data held in other formats (Excel, CLO notes etc) using a variety of metadata element sets must be supported.
- (d) Allows Administrator-assigned ‘identification tag’s’/symbols to be linked to records to identify them as being held in or having been exported from the system they were created in.
- (e) Display this ‘identification tag’ in any search results lists.
- (f) Enable other functionality to be defined according to the system that the records are held in or have been migrated from. For example, the folder/classification structure or level and format of description in legacy systems may vary from current systems and impact on the results of other system operations or searches.
- (g) Support the importation or direct entry of metadata of manual records systems or individual physical records. These which have a variety of metadata element sets and are in a variety of formats, including card indexes, file registers, Solicitor-General records etc.

3. CLASSIFICATION

3.1 Classification Scheme

- (a) Support and be compatible with Crown Law’s classification schemes, including the Client Matter system and the Corporate Filing system. This will require support of

hierarchical classification systems represented by a minimum of three hierarchical levels and allow for an unlimited number of levels.

- (b) Support the initial construction of a classification scheme, and allow naming conventions to be defined, at the time the electronic records management system is configured, so that they are in place before electronic records are captured or imported.
- (c) Allow for the allocation of structured numeric or alphanumeric reference codes (i.e. a matter number or a code representing the hierarchical level of the Corporate classification) to each electronic folder (at any level) and to allocate a text title for each electronic folder (at any level). The codes should be unique within the classification scheme and it must be possible to apply both identifiers separately or together.
- (d) Be able to define folders, record groupings or volumes and record groupings in the classification scheme/folder structure that consist of physical records only (possibly created without involvement of a business application, such as Solicitor-General records) and those that consist of both physical and electronic records. Both kinds of record must be able to be managed in an integrated way.

Examples:

Physical only:	Corporate files
Physical and Electronic:	Client/Matter records
	Draft Bills, invoices etc

- (e) Enable all business critical systems that create records to be mapped to the records management metadata model/folder structure.
- (f) Support the definition and simultaneous use of multiple classification schemes to enable integrated management of Crown Law's current classification systems and legacy classification systems.
- (g) Support browsing and graphical navigation of folders and the classification scheme structure.
- (h) Support the use of controlled vocabulary/thesaurus terms and relationships and enable these terms to be linked to the classification scheme. If possible the terms should be drawn from an ISO 2788- or ISO 5964-compliant thesaurus.

3.2 Aggregations (including Volumes)

- (a) Support records management metadata for folders (at any level including volume) and hierarchical levels in the classification scheme.
- (b) Allow Records Administrators to create folders at any level within any folder in the folder structure.
- (c) Allow Records Administrators to create new folders at the highest level in the folder structure/classification scheme (for example, at the business function level).

- (d) Allow Records Administrators to add (open) electronic volumes to any electronic folder that is not closed.
- (e) Allow a Records Administrator to re-open a previously closed volume temporarily for the addition of records, and subsequently to close that volume again. Any volume that has been temporarily re-opened to should automatically close if the Administrator who opened it logs off.
- (f) Restrict to Administrators the ability to move folders (at any level including volumes) and individual records.
- (g) Allow the Administrator to enter the reason for the reclassification of folders (including volumes) and individual records.
- (h) Allow an electronic folder to be closed by a specific Administrator procedure, and must restrict this function to an Administrator.
- (i) Support the concept of open and closed volumes for electronic folders at the lowest levels of the folder structure and allow for multiple electronic volumes within a folder corresponding to the physical volumes.
- (j) Allow only the most recently created correspondence volume within a folder to be open and prevent users from adding electronic records to any closed volume.
- (k) Allow a defined set of metadata to be applied at the volume level.
- (l) Record the date of opening and date of closing of a volume as separate elements in the volume's metadata.
- (m) Support the creation of an initial set of open volumes according to Records Administrator defined templates based on parameters such as folder structure, business function or activity, work group/work type etc, when a workspace is created.
- (n) Support integrated management of the physical and electronic volumes by ensuring that they cover the same periods of time.
- (o) Support the creation of volumes by Records Administrator defined record types and allow unique identifiers to be assigned at the record type level and an overall sequential unique identifier to be applied across all volumes within a folder. Examples of record types might be correspondence, pleadings, discovery documents, record of inquiry etc.
- (p) Allow for additional record type volumes to be created within a matter.
- (q) Support automatic closure of a volume of an electronic folder according to specified criteria defined at configuration. The criteria options should include 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 and the size of a volume.
- (r) Enable users to create cross-references between related folders (at any level including volumes) or between folders and individual records

3.3 Classification Scheme Maintenance

- (a) Allow the position of an electronic folder (including volumes) in the folder structure/classification scheme to be changed while ensuring that all electronic records already associated with that folder remain allocated to it.

For example:

If a Matter, containing multiple documents possibly organised in separate volumes, was moved in the structure from under one Client to another, all electronic documents that were associated with the matter under the original Client will still be associated to it under the new Client after the move.

- (b) Allow users to re-classify an electronic record to a different open volume of an electronic folder and allow Administrators to re-classify records to either open or closed volumes.
- (c) Be able to produce a report listing folders, structured to reflect the classification scheme/folder structure, for all or part of the classification scheme/folder structure.
- (d) Where appropriate provide a warning if an attempt is made to capture a record which is incomplete or inconsistent with its position in the folder structure or its relationship to other records.
- (e) Not impose any practical limit on the number of folders that can be defined at any level.

4. IDENTIFICATION

- 4.1 Allocate an identifier, which is unique within the system, to each record when it is captured.
- 4.2 Associate a unique identifier with each:
 - (i) Record;
 - (ii) Record extract;
 - (iii) Folder (at any level including volume)
- 4.3 Ensure that the identifiers are unique within the folder (at any level) within which the record appears and are stored as one of the metadata elements for that folder (at any level).
- 4.4 Generate unique identifiers automatically and prevent users from inputting the unique identifier manually, and from being able to modify it.
- 4.5 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 sequence of identifiers of the volume and electronic folders above the record in the classification scheme/folder structure.
- 4.6 Where the unique identifiers are based on sequential numbering, the electronic records management system should automatically generate the next sequential number

available at that position within the classification scheme/folder structure for each new electronic folder.

5. MAINTAINING RECORDS

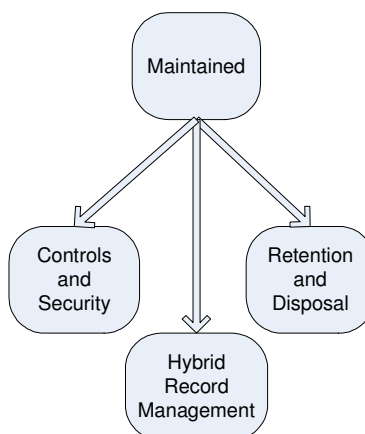


Figure 8 – Records maintenance process

6. CONTROLS AND SECURITY

6.1 Access

- (a) Control functions should be definable for roles as well as for users.
- (b) Allow for groups of users that are associated with a folder (at any level) to be set up and for users' access to parts of the list of folders (at any level) to be limited.
- (c) Allow a user to be a member of more than one group.
- (d) Never include any record that the user does not have the right to access, in a list of full text or other search results.
- (e) Restrict access to system functions according to user's role and system administration controls.
- (f) Include features to control and record access to physical folders, including controls based on security category, which are similar to the features for electronic folders.
- (g) Never allow a search or retrieval function to reveal any information to a user (metadata or record content) that the access and security settings are intended to hide from that user.
- (h) Provide for the following options (selectable at configuration time) whenever a user requests access to, or searches for, a record, volume or folder (at any level) that they do not have the right to access:
 - (i) display title and records management metadata;
 - (ii) display the existence of an folder (at any level) or record (i.e. display its file or record number) but not its title or other records management metadata;
 - (iii) do not display any record information or indicate its existence in any way.

- (i) If the electronic records management system allows users to make unauthorised attempts to access folders (at any level and their volumes) or records, the electronic records management system must log all unauthorised attempts to access folders (at any level 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.
- (j) Allow all records management metadata for every record to be viewed by users, subject to access rights for individuals or groups of users.
- (k) Support Administrator-defined matter status options in addition to the current options of active, stopped and closed, such as 'archived' 'transferred' 'destroyed' etc.
- (l) Allow only Administrators access to change the matter status.

6.2 Public Access Restrictions

- (a) Allow a public access restriction status of "open" or "restricted" to be applied as part of the metadata of all individual records and/or folders at any level including volume. If a higher level in the folder structure is restricted, all folders or records associated below it are to receive a "restricted" access classification.
- (b) Allow information related to the restriction category such as the restriction definition, access conditions and privileged access request procedures to be recorded and for this to be viewable by users.
- (c) Allow for a restriction to be applied to a record or folder at any level at any time, whether the record is open or closed or has been subject to a disposal process.
- (d) Allow additional restriction statuses and categories defined by the Records Administrator to be added at later dates.
- (e) Prevent any restricted record or folder from being publicly available through Crown Law systems.
- (f) Provide a facility for applying public access restriction classifications to metadata associated with records, so that descriptions of records that contain sensitive information can be withheld from public access.
- (g) Allow only Records Administrators or specified users or groups to apply public access restrictions to records or folders.

6.3 User Access

- (a) Provide a single point of access for users undertaking records management functions requiring data entry or transactions, such as volume creation, volume closing, record tracking etc.
- (b) Enable decentralisation of some functions including record creation, volume creation, volume closing, tracking functionality, some location management functionality, to reflect the Crown Law structure of records management activity.

6.4 Audit Trails

- (a) Keep a clear trace of the status of reclassified folders at any level (including volumes) prior to their reclassification in the records management metadata, so that their entire history can be easily identified.
- (b) Be capable of creating an unalterable audit trail of records management actions that are taken upon records, folders (at any level), or the classification scheme/folder structure. The audit trail should include the following records management metadata elements: type of records management action; user initiating and/or carrying out the action; date and time of action.
- (c) Be capable of capturing and storing in the audit trail information about the following actions:
 - (i) the date and time of capture of all electronic records.
 - (ii) re-classification of an electronic record in another electronic volume.
 - (iii) re-classification of an electronic folder (at any level) in the classification scheme/folder structure.
 - (iv) any change to the disposal authority of an electronic folder (at any level).
 - (v) any change made to any records management metadata associated with folders (at any level including volumes) or electronic records.
 - (vi) date and time of creation, amendment and deletion of records management metadata.
 - (vii) changes made to the access privileges affecting an electronic folder (at any level).
 - (viii) electronic record or user; export or transfer actions carried out on an electronic folder (at any level).
 - (ix) date and time at which a record is displayed, printed or rendered.
 - (x) disposal actions on an electronic folder (at any level) or record.
- (d) The electronic records management system should track events without manual intervention, and store in the audit trail information about them. The audit trail information should be maintained for as long as required by disposal authorities.
- (e) Provide an audit trail of all changes made to electronic folders (at any level including volumes); individual electronic records; and records management metadata associated with any of the above.
- (f) Provide an audit trail of all changes made to administrative parameters (for example, changes made by the Administrator to a user's access rights).
- (g) 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. This feature should be able to be easily used by Public Records Act Auditors.
- (h) Be able to export audit trails for specified records and selected groups of records without affecting the audit trail stored by the electronic records management system.
- (i) Be able to capture and store violations (i.e. a user's attempts to access a record or folder to which he or she is denied access), and (where violations can validly be attempted) attempted violations, of access control mechanisms. This feature should be controllable so that the Administrator can specify security categories.

- (j) Be able to record in the audit trail all changes made to metadata references to physical or hybrid (physical and electronic) folders and records.
- (k) Store in the audit trail all decisions taken by the Records Administrator reviewer during disposal process reviews.

6.5 Backup and Recovery

- (a) Provide automated backup and recovery procedures that allow for regular comprehensive backup of all or selected classes, folders (at any level), records, records management metadata and administrative attributes of the electronic records management system repository.
- (b) 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.
- (c) Allow vital records and other records to be restored in separate operations.

6.6 Tracking Record Movement

- (a) Provide a tracking feature to monitor and record information about the location and movement of both electronic and physical folders (at any level in the folder structure).
- (b) Record information about movements in a audit trail including:
 - (i) unique identifier of the folder (at any level) or record;
 - (ii) home location
 - (iii) current location
 - (iv) a defined number of previous locations (to be defined by the Records Administrator and searchable)
 - (v) date item sent/moved from location;
 - (vi) date item received at location (for transfers);
 - (vii) user responsible for the move (where appropriate).
- (c) Support tracking of physical folders by the provision of request, check-out, and check-in facilities that record the current location of the item concerned, and display this information if the item is requested by another user.
- (d) Enable the request system to be operated in a decentralised way so for example, Secretaries can operate it within teams, Litigation Services staff can operate it for client and Archives NZ loan records, and Records staff can operate it for records stored in central systems or off-site.
- (e) The request facility should enable a user to enter a date that the physical folder(s)/records is required, and generate a consequent message for transmission to the current holder of that physical folder(s)/record or the Records Administrator alerting them to the request.
- (f) Provide the ability for users to tag the records/volumes they require from lists of search results and compile them into a list of requests that they can then submit through the system.

- (g) Support the migration or capture of location management data currently contained in business applications into the electronic records management system. This includes data in the “File no.” field and AR Notes field in the Practice Management system.
- (h) Support a bar coding tracking system to automate tracking the movement of physical records.
- (i) Allow multiple formats of bar codes to be printed and recognised so that bar codes supplied by Crown Law’s off-site storage provider; and the original bar codes of records on loan from clients, Archives New Zealand or from various off-site storage facilities; and inherited records can be used in the system.
- (j) Support the printing and recognition of bar codes for physical objects (e.g. documents, folders and other containers) and compatibility with auxiliary bar code recognition equipment (hand held units, multiple sites etc).

6.7 Authenticity

- (a) Restrict access to system functions according to user’s role and strict system administration controls.
- (b) Prevent any unrecorded change to the content of the electronic record by users and Administrators.

6.8 Data Authenticity

- (a) The content of any record must not be alterable by any user or administrator once it has been captured within the electronic records management system and has been certified as the final version.
- (b) Any metadata automatically extracted from the software application that created the record must not be alterable.
- (c) Ensure that only authorised users and Administrators can change the content of any additional records management metadata elements captured.
- (d) Ensure that the text of an email, its transmission details, and the subject line of the email cannot be amended in any way once the email has been captured. Note: An additional record title for the email can be entered to increase accessibility through searching.
- (e) For each action undertaken on a record the following minimum records management process metadata must be maintained: date of the action, the identification of the person undertaking the action, what action was taken.

6.9 Government Security Classifications

- (a) Allow security classifications to be assigned to records or folders (at all levels including volumes).
- (b) Allow one of the following security clearances to be assigned to users:
 - (i) Unclassified;
 - (ii) In Confidence (policy and privacy);

- (iii) Sensitive (policy and privacy);
 - (iv) Restricted (national security information);
 - (v) Confidential (national security information);
 - (vi) Secret (national security information);
 - (vii) Top Secret (national security information).
- (c) Deny users access to electronic records or folders at any level (including volume) that have a security classification higher than their security clearance.
 - (d) Automatically assign a default value of 'Unclassified' to a folder (at any level) or record not allocated any other security category.
 - (e) Ensure that a hybrid physical folder is allocated the same security category as an associated hybrid electronic folder. (see Hybrid Record Management).
 - (f) Be able to determine the highest security category of any record in any folder through one simple enquiry.
 - (g) Support routine, scheduled reviews of security classifications.
 - (h) Prevent an electronic folder from having a lower security classification than any electronic record within that folder.
 - (i) Enable the ERMS's security subsystem to work effectively together with general security products.

7. RETENTION AND DISPOSAL

7.1 Destruction Control

- (a) Prevent the destruction or deletion of any record or electronic folder (at any level) by any user.
- (b) Enable destruction by the Records Administrator of records or folders (at any level) according to approved disposal authorities and procedures.
- (c) Ensure that records that consist of multiple components are disposed of as single units.

7.2 Disposal Authorities

- (a) Provide a function that specifies disposal authorities and allows them to be assigned to any record or folder (at any level including volume).
- (b) Support a default setting that ensures that every record in a folder (at any level) is governed by the disposal authority(s) associated with that folder.
- (c) Enable a disposal authority to be assigned to a folder (at any level) that over-rides the disposal authority assigned to its 'parent' folder.
- (d) Each disposal authority should include a disposal authority decision number, a disposal authority title, a disposal action, Crown Law on-site retention period, Crown Law off-site retention period, and an overall retention period.

- (e) In cases of digitisation, enable links between disposal authority actions for source records and corresponding digitised records to be established and ensure that the retention period for the digitised record is at least as long as that for the source record.
- (f) Be capable of associating more than one disposal authority with any folder (at any level) or class of a classification scheme/folder structure.

7.3 Disposal Actions

- (a) Allow at least the following decisions for each disposal authority:
 - (i) retain indefinitely;
 - (ii) present for review at a future date;
 - (iii) destroy at a future date;
 - (iv) transfer at a future date;
- (b) Automatically track retention periods that have been allocated to each folder (at any level) and initiate the disposal process once the end of the retention period is reached.
- (c) Allow retention periods for each disposal authority to be specified for a future date, with options:
 - (i) A defined period of time after the folder (at any level) is opened;
 - (ii) A defined period of time after the folder (at any level) is closed;
 - (iii) A defined period of time since the most recent record has been assigned to the folder (at any level);
 - (iv) A defined period of time after a specific event (event to be identified in the schedule, and will be notified to the electronic records management system by the Administrator rather than being detected automatically by the electronic records management system);
 - (v) Specified as “indefinite” to indicate long-term preservation of the records.
- (d) Retention periods should be able to be set from a minimum of one month to an indefinite period.

7.4 Disposal Review Process

- (a) Support the review process by presenting electronic folders (at any level) along with their records management metadata and disposal authority information to be reviewed, in reports to the Records Administrator (reviewer).
- (b) If more than one disposal authority is associated with a folder (at any level including volume), the electronic records management system must 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.
- (c) Automate disposal review reporting actions.
- (d) Allow the reviewer to take at least any one of the following actions for each folder (at any level) or record during review:
 - (i) mark the folder/record for destruction;

- (ii) mark the folder/record for transfer;
 - (iii) change the disposal authority (or assign a different schedule) so that the folder/record is retained and re-reviewed at a later date defined by the Records Administrator.
- (e) Allow the reviewer to enter comments into the folder or record's metadata to record the reasons for the review decisions.
- (f) Alert the Records Administrator to folders (at any level)/records due for disposal before implementing disposal actions; and on confirmation from the Administrator the electronic records management system must be capable of initiating the disposal actions specified. All disposal actions carried out should be automatically reported to the Records Administrator.
- (g) Tag records covered by Deferred Transfer Agreements, record the relevant Disposal Authority reference, and deferred transfer period and notify the Records Administrator a defined period before the deferment period is due to expire.
- (h) Support the retention of defined metadata for records (whether electronic, a record controlling a physical or hybrid record, or a digitised record etc) along with the associated disposal action once the action has been carried out.
- (i) Allow sets of processing rules to be defined and applied as an alerting facility to specified folders (at any level) prior to initiation of a disposal process.
- (j) Provide the option of allowing electronic records or folders (at any level) that are being moved between folders/folder levels by the Administrator to have the disposal authority of the new folder/folder level, replacing the existing disposal authority(s) applying to these records.
- (k) Be able to specify the frequency of a disposal authority report, the information reported and highlight exceptions such as overdue disposal.
- (l) Alert the Records Administrator if an electronic folder (at any level) that is due for destruction is referred to in a link from another folder and pause the destruction process to allow confirmation by the Records Administrator to proceed with or cancel the process. A report detailing the folder (at any level) or record(s) concerned and all references or links for which it is a destination should be generated.
- (m) Support reporting and analysis tools for the management of retention and disposal authorities by the Administrator, including the ability to:
 - (i) list all disposal authorities;
 - (ii) list all electronic folders (at any level) to which a specified disposal authority is assigned;
 - (iii) list the disposal authority(s) applied to all folders (at any level) below a specified point in the hierarchy of the classification scheme;
 - (iv) identify, compare and review disposal authorities (including their contents) across the folder structure/classification scheme;
 - (v) identify formal contradictions in disposal authorities across the folder structure/classification scheme.
- (n) Support the ability to utilise a workflow facility to support the scheduling, review and export/transfer process, by tracking the progress or status of the review, details of

reviewer and date; records awaiting disposal as a result of a review decision; and progress of the transfer process.

- (o) Be able to collect statistics of review decisions made in a given period and provide tabular and graphic reports on the activity.

7.5 Metadata

- (a) The ERMS must allow Disposal Authorities and Disposal Actions to be applied to metadata.
- (b) The ERMS must ensure that metadata cannot be destroyed without Records Administrator confirmation as part of the Disposal Review process.
- (c) After disposal actions on a record are carried out (including transfer and destruction), the following metadata must be retained for at least the life of the system:
 - (i) point of capture metadata including a unique identifier, a title, date of creation, who created the record, what business is being conducted, and the creating application
 - (ii) the circumstances of the record's disposal.
 - (iii) the date the action took place.
 - (iv) the authority governing record's destruction.
 - (v) the person undertaking the action.

7.6 Transfer and Destruction

- (a) Provide a well-managed process to transfer records to another system or to a third party organisation.
- (b) Include all folders, volumes, records and associated records management metadata folders whenever an electronic records management system transfers any level of folder, record or volume from the system.
- (c) Be able to transfer or export a folder (at any level) in one sequence of operations so that:
 - (i) the content and structure of its electronic records are not degraded;
 - (ii) all components of an electronic record (when the record consists of more than one component) are exported as an integral unit;
 - (iii) all links between the record and its records management metadata are retained;
 - (iv) all links between electronic records, volumes and folders/record groupings are retained.
- (d) Be able to include a copy of all the audit trail data associated with the records, volumes and folders (at all levels) that are transferred or exported from an electronic records management system.
- (e) Produce a report detailing any failure during a transfer, export or destruction. The report must identify any records identified for transfer that have generated processing errors, and folders (at any level) or records that are not successfully transferred, exported or destroyed.

- (f) Retain copies of all electronic folders (at any level) and their records that have been transferred, at least until a successful transfer is confirmed.
- (g) Be able to continue to manage records and folders (at any level) that have been exported from the electronic records management system to other forms of storage media.
- (h) Have the ability to retain records management metadata for records and folders that have been destroyed or transferred.
- (i) Automate destruction actions and provide integrated facilities for exporting records and records management metadata.
- (j) Migration of digital records must support the identification of which record objects and associate metadata are required to enable Crown Law to continue to access the authentic digitised record.
- (k) The original metadata for digital records must be migrated into any system replacing the one in which the digital image was originally managed
- (l) The storage environment must support the retrieval of the record for as long as required.
- (m) Provide a utility or conversion tool to support the conversion of records marked for transfer or export into a specified format for file transfer or export.
- (n) Provide the ability to add user-defined records management metadata elements required for archival management purposes to an electronic folder selected for transfer. These will include Archives New Zealand office, transfer and item reference codes.
- (o) Provide the ability to sort electronic folders selected for transfer into ordered lists according to user-selected records management metadata elements.
- (p) 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.
- (q) Where hybrid folders are to be transferred, exported or destroyed, the electronic records management system should require the Records Administrator to confirm that the physical part of the same folder has been transferred, exported or destroyed before transferring, exporting or destroying the electronic part.

8. HYBRID RECORD MANAGEMENT

8.1 Management of Physical and Electronic Records

- (a) Allow a physical folder that is associated with an electronic folder as a hybrid record to use the same title and numerical reference code, but with an added indication that it is a hybrid physical folder.
- (b) Allow a different records management metadata element set to be configured for physical and electronic folders. Physical folder metadata must include information on the physical location of the physical folder.

- (c) Ensure physical folder search results display the records management metadata for both electronic and physical record that are associated as a hybrid.
- (d) Support the management of physical records created as a result of business activities undertaken using business applications. For example, records produced based on data in the Practice Management system by allowing the capture of descriptive metadata relating to them.
- (e) Maintain access to the electronic record content, including the ability to display and print it, and maintenance of its structure and formatting, over time and through generations of office application software.

8.2 Retention and Disposal of Physical and Hybrid records

- (a) Support the allocation of disposal authorities to every physical folder (at any level) in the classification scheme. The authorities must function consistently for electronic and physical folders, notifying the Administrator when the disposal date is reached, but taking account of the different processes for disposing of electronic and physical records.
- (b) Support the application of the same disposal authority to both the electronic and physical folders that make up a hybrid folder.
- (c) Be able to apply any review decision made on a hybrid electronic folder to a physical folder it is associated with.
- (d) Include a configurable option to prevent any record, once captured, from being deleted or moved by any Administrator or user without affecting transfer or destruction operations in accordance with disposal authorities.
- (e) If the system allows the Records Administrator to delete folders (at any level), volumes and records the electronic records management system must:
 - (i) record the deletion comprehensively in the audit trail;
 - (ii) produce an exception report for the Administrator;
 - (iii) delete the entire contents of a folder or volume when it is deleted;
 - (iv) 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 one of which is being deleted);
 - (v) inform the Administrator, of any links from another folder (at any level), or record to an folder or volume which is about to be deleted, and request confirmation before completing the deletion;
 - (vi) maintain complete integrity of the records management metadata at all times.
- (f) Support review decisions being applied to any physical folder by notifying the Administrator of necessary actions to be taken on the physical folders when they are in groups of folders covered by a disposal authority.
- (g) Be able to export and transfer the records management metadata of physical records and folders.

8.3 Off-site Storage

- (a) Support the functionality currently covered by the Off-site Storage Retrieval Register, by providing the ability to record requests and their status. Information required to be captured includes Requestor name, Counsel name, Team, Date Requested, Who ordered, Box number, Box bar code number, item bar code, Date received, Date returned, and comments.
- (b) Ensure that bar codes provided by our Off-site storage provider can be used within the system to track items, records and boxes when on-site.
- (c) Provide a practical solution for the batch upload of data from within the system to our Off-site storage providers system; i.e. Enable data within the records management system to be copied and exported into a third party system. (What implications are there likely to be for all parties and what would we need to explore with our storage providers to implement this?)

8.4 On-site Storage

- (a) Enable lists of records in location order and lists of locations in order to be printed.
- (b) Support a bar code tracking system that identifies storage systems, their components, shelves and boxes and allows for another name to be applied to each of these in addition to the bar code.
- (c) Support secure storage management by allowing the recording of an indicator of the level of security associated with the physical item stored, and by requiring Records Administrator confirmation of access to securely stored items.
- (d) Provide a facility to allow the Administrator to define of storage systems and equipment assigned to each user, office, workstation, group or area; record system form and capacity; link to location identifications; and enable the Administrator to assign these resources.
- (e) Ability to define and report on the contents of storage allocations.

8.5 Format and Media

Allow customised management of records in various formats and media including paper, audio and video; photographs; microforms; scanned documents and images by enabling formats and media to be documented and managed separately.

9. CLIENT AND ARCHIVES NEW ZEALAND LOAN MANAGEMENT

9.1 General

- (a) Support the equivalent of the current loan register which records the details of each record or item received on loan, by team, including:
 - (i) the client matter reference;
 - (ii) matter description;
 - (iii) name of agency file borrowed from (usually a client or Archives New Zealand);

- (iv) file reference and description (including Archives NZ production number, Archives NZ codes, client/original file reference codes, volume number, record title or description, discovery reference, received, location, last sighted inspection/audit);
 - (v) returned details;
 - (vi) related correspondence;
 - (vii) notes;
 - (viii) Signature box number;
 - (ix) Signature Cannae file number;
 - (x) Signature Cannae file status
- (b) Allow the record loan period expiry to be recorded and issue reminder notifications to the Administrator/Requestor when the end of the loan period is reached.
 - (c) Provide links to matters that records are loaned in relation to, so that it is possible to have multiple links and document multiple records loaned for individual matters.
 - (d) Enable the generation and printing of receipt and return letters utilising the record/item description metadata captured and as part of this process be able to select the set of records/items involved.
 - (e) Enable the generation and printing of reports of selected records/items on loan.

9.2 Location Management

- (a) Allow for temporary home locations to be assigned and locations to be tracked for all records/items on loan, as for Crown Law record location management.
- (b) Allow for the location record for individual or selected groups of items on loan to be updated on confirmation by the Records Administrator that a return letter is final, correct, and that returned records have been receipted.
- (c) Support the assignment of bar codes to records on loan, and enable bar code tracking of them as for Crown Law record location management.
- (d) Enable loan records to be linked with the matters they relate to so that users can access the details of loans relating to a particular matter from the workspace for that matter.

9.3 Audits/Inspections

- (a) Enable generation and printing of reports of current locations of all items/records due for inspection.
- (b) Allow for loan record location movement to be tracked during the inspection process.
- (c) Allow the bulk update of the set of records/items involved in an audit inspection with information relating to the audit inspection.
- (d) Allow for the tagging of records/items as having been temporarily returned to Archives NZ for inspection.

10. SEARCH RETRIEVE AND RENDER

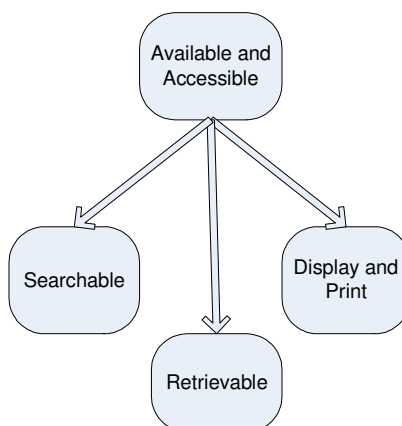


Figure 9 – Accessibility process

10.1 Searching

- (a) Provide a flexible range of search and retrieval functions operating on the records management metadata related to every level of folder and on the contents of the records. These should include all user-defined search parameters and searching and retrieval of individual records or groups of records; any level of folder including volumes; and/or their metadata.
- (b) Records that are made up of multiple components should be retrieved and displayed, as single units.
- (c) Allow users to set up a single search request with combinations of records management metadata and/or record content.
- (d) Provide searching tools that cover the following techniques:
 - (i) Free-text searching of combinations of record and folder metadata elements and record content;
 - (ii) Boolean searching of metadata elements.
 - (iii) provide for “wild card” searching of metadata that allows for forward, backward and embedded expansion.

and if possible:

- (iv) Provide free-text and metadata searches in an integrated and consistent manner.
- (v) Provide concept searches through the use of a thesaurus incorporated as an online index.
- (vi) Provide word proximity searching that can specify that a word must appear within a given distance of another word in the record to qualify as a search result.
- (vii) Allow users to save and re-use queries
- (viii) Allow users to refine (i.e. narrow) searches.

- (e) Allow searching within a single folder at any level or across more than one folder or level of folders.
- (f) Be able to search for, retrieve, and display all the records and metadata relating to an electronic folder (at any level), or volume, as a single unit.
- (g) Be able to search for, retrieve and print an electronic folder (at any level) by the defined record naming conventions, including: name, identifier, classification code.
- (h) Where a graphical user interface (GUI) is used, the electronic records management system must provide a browsing mechanism that enables graphical, or other display browsing techniques, at any level of folder.
- (i) Allow integrated searching across all records and folders, regardless of the business application that the records might have been created in or captured from.
- (j) Support the selection, retrieval and display of electronic folders (at any level) and their contents through browsing and navigation of the folders and classification scheme.
- (k) Have integrated search facilities that appear the same to users for all levels of the classification scheme.
- (l) Present seamless functionality when searching across electronic, physical, and hybrid folders (at any level).
- (m) Allow the records management metadata of any object (such as record, volume, or folder/record grouping) 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.
- (n) Provide relevance ranking of the search results.
- (o) Allow users who are viewing or working with a record or folder (at any level), whether as the result of a search or otherwise, to find information about the next-higher level of folder of records easily and without leaving or closing the record.

10.2 Retrieving records

- (a) Allow records and folders (at any level) featured in the search results list to be selected, then opened (subject to access controls) by a single click or keystroke.
- (b) Allow users to retrieve folders (at any level) and records directly through use of a unique identifier.
- (c) 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 records management metadata and access controls over the two items.

10.3 Displaying

- (a) Allow all records management metadata for every record to be viewed by users, subject to access rights for individuals or groups of users.
- (b) Display the total number of search results on the user's screen and allow the user to then display the results list, or refine the search criteria and issue another request.

- (c) Enable the creation of forms and templates.
- (d) Provide search results in display formats configurable by users or Administrators. They should allow users to:
 - (i) select the order in which the search results are presented;
 - (ii) specify the number of search results displayed on the screen;
 - (iii) set the maximum number of search results;
 - (iv) save the search results;
 - (v) choose which records management metadata fields are displayed in search result lists.
- (e) Display records that the search request has retrieved without loading the associated application software.
- (f) Be able to display all the types of electronic records created or held by Crown Law in a way that preserves all the information in the record, including features of visual presentation and layout produced by the generating application package, and which displays all the components of the electronic record together.

10.4 Printing

- (a) Provide users with flexible options for printing records and their relevant records management metadata, including the ability to print a record or multiple records with records management metadata specified by the user and printing records management metadata for a folder or folders (at any level).
- (b) Allow the user to be able to print out a summary list of selected records (e.g. the contents of a folder), consisting of a user-specified subset of records management metadata elements (e.g. Title, Author, Creation date) for each record.
- (c) Allow users to print the results list from all searches.
- (d) Be able to print all the types of electronic records created or held by Crown Law. Printing must preserve the layout produced by the generating application package(s) and include all (printable) components of the electronic record.
- (e) Allow all records in a folder (at any level) to be printed, in the sequence specified by the user, in one operation.
- (f) Enable forms and templates (including for Disposal Schedules, Loan receipt and return form letters, appraisal review lists, shelf/location lists, etc) to be printed.
- (g) Enable production of file labels including the front cover label, tab label, transit card label and bar code labels, shelf identifiers, bar codes (boxes, files, users, locations etc) in user defined quantities and ability to save generated labels for future additional printing. These should be able to be generated according to Administrator defined templates.
- (h) Enable the production of location labels based on location identification metadata including bar codes.

- (i) Allow the creation of records inventories, involving searching, displaying, sorting and printing on Records staff-defined metadata. These will include box content inventories, appraisal list inventories, transfer lists etc

10.5 Other

Include features for rendering records, such as audio, visual files, and database files, that cannot be meaningfully printed to an appropriate output device.

11. ADMINISTRATION

11.2 General Administration

Capture

- (a) Allow Administrators to make bulk changes to the classification scheme, ensuring all records management metadata and audit trail data are handled correctly and completely at all times, in order to make the following kinds of office organisational change; including division, combination, movement or re-naming of teams.
- (b) Allow an administrator to un-register a captured record if required, to allow finalisation of the record profile. Any temporary un-registration should be visible in an audit trail.
- (c) Where unique identifiers are automatically generated, the electronic records management system should allow the Administrator to specify the starting number (e.g. 1, 10, 100) and increment (e.g. 1, 10) to be used in all cases when the system is configured.
- (d) Allow Records Administrators, and any users they allocate the privilege to, to indicate that selected records are considered to be 'vital records' that are absolutely necessary to Crown Law's ability to continue its business and to protect its financial and legal interests in the event of an emergency or disaster.

Retention and Disposal

- (a) Be able to restrict the setting up and changing of disposal authorities to the Records Administrator(s) only.
- (b) Allow the Records Administrator(s) to define and store a standard set of customised standard disposal authorities.
- (c) Automatically record and report all disposal actions to the Records Administrator(s).
- (d) Allow the Administrator to change any disposal authority allocated to any folder (at any level) at any point in the life of that folder.
- (e) Allow the Administrator to change the authority(s) associated with a folder (at any level) at any time.
- (f) Allow the Administrator to specify a subset of folder metadata that will be retained for folders that are destroyed, transferred out or moved offline.
- (g) Alert the Administrator to the existence and location of any hybrid physical folder associated with a hybrid electronic folder that is to be exported or transferred.

- (h) Communicate any errors encountered in saving data to storage media.
- (i) Allow the Records Administrator to extract statistical data relating to the disposal process and actions.
- (j) 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.

Searching and Printing

- (a) Allow Administrators to configure and change the search fields to: specify any element of record, volume and folder records management metadata, and optionally full record content, as search fields; change the search field configuration.
- (b) Allow the Administrator to specify that all printouts of records have selected records management metadata elements appended to them, e.g. title, registration number, date, security category.
- (c) Allow Administrators to print
 - (i) the thesaurus;
 - (ii) any and all administrative parameters;
 - (iii) disposal authorities;
 - (iv) the classification scheme;
 - (v) audit trails;
 - (vi) the file list;

Information Technology Administrator functions

- (a) Maintain internal integrity (relational integrity or otherwise) at all times, regardless of: maintenance activities, other user actions, or failure of system components. It must be impossible for a situation to arise where any user action or any software failure results in an inconsistency within the electronic records management system or its database.
- (b) The system needs to provide reporting tools for the provision of statistics to the Records Administrator on aspects of activity within the classification scheme, including the numbers of electronic folders (at any level including volumes) or records created, closed or deleted within a given period.
- (c) Allow the Administrator to limit access to records, folders (at any level) and records management metadata to specified users or user groups.
- (d) Allow the Administrator to attach to the user profile attributes that determine the features, records management metadata fields, records or folders (at any level) to which the user has access. The attributes of the profile will:
 - (i) prohibit access to the electronic records management system without an accepted authentication mechanism attributed to the user profile;
 - (ii) restrict user access to specific records or folders (at any level);
 - (iii) restrict user access according to the user's security clearance
 - (iv) restrict users access to particular features (e.g. read, update and/or delete specific records management metadata fields);

- (v) deny access after a specified date; allocate the user to a group or groups.
- (e) Allow only Administrators to set up user profiles and allocate users to groups.
- (f) 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.
- (g) Allow the Administrator to schedule backup routines by:
 - (i) specifying the frequency of backup;
 - (ii) selecting classes, folders (at any level) or records to be backed up;
 - (iii) allocating storage media, system or location for the backup (e.g. offline storage, separate system, remote site).
- (h) Allow only the Administrator to restore from electronic records management system backups. Full integrity of the data must be maintained after restoration.
- (i) Allow only the Administrator to roll-forward the electronic records management system from a backup to a more recent state, maintaining full integrity of the data.
- (j) Allow Administrators to retrieve, display and re-configure system parameters and to reallocate users and functions between user roles.
- (k) Provide backup facilities so that records and their records management metadata can be recreated using a combination of restored backups and audit trails.
- (l) Provide recovery and rollback facilities in the case of system failure or update error, and must notify Administrators of the results. The EMRS must allow Administrators to 'undo' a series of transactions until a status of assured database integrity is reached, when error conditions arise.
- (m) 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.
- (n) Support the movement of users between Crown Law teams.
- (o) Allow the definition of user roles, and must allow several users to be associated with each role.
- (p) 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 records management system must ensure that this selection and all changes to it are stored in the audit trail.

11.2 Reporting

- (a) Provide flexible reporting facilities for the Administrator. They must include, at a minimum, the ability to report the following: numbers of folders (at any level), volumes and records; transaction statistics for folders (at any level), volumes and records; activity reports for individual users.

- (b) Allow Administrators to report on audit trails based on selected folders (at any level); volumes; records; users or time periods.
- (c) Allow Administrators to request regular periodic reports and one-off reports.
- (d) Be able to provide reports for actions on records and folders (at any level) organised by record or folder (at any level); by user; or in chronological sequence.
- (e) Be able to provide reports for actions on folders (at any level) and records organised by workstation and by network address.
- (f) Allow Administrators to report on audit trails based on selected: security categories; user groups; other records management metadata.
- (g) Include features for sorting and selecting report information.
- (h) Include features for totalling and summarizing report information.
- (i) Allow Administrators to restrict users' access to selected reports.

11.3 Altering and deleting records

- (a) 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. If deletion by the Administrator is allowed the system must:
 - (i) record the deletion comprehensively in the Audit trail;
 - (ii) produce an exception report for the Administrator;
 - (iii) delete the entire contents of an aggregation or volume when it is deleted;
 - (iv) 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, one of which is being deleted);
 - (v) 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;
 - (vi) maintain complete integrity of the recordkeeping metadata at all times.
- (b) Allow the Records Administrator to change any user-entered records management 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.
- (c) Allow the Administrator to alter the security category of individual records, all records within a folder (at any level), or parts of the folder structure in one operation. The electronic records management system must provide a warning if any records are having their security category lowered, and await confirmation before completing the operation.
- (d) Record full details of any change to security category in the records management metadata of the record, volume or folder at any level affected.

11.4 Redacting Records

- (a) Allow Administrators and authorised users 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 document.
- (b) Record the creation of extracts in the record's metadata, including the date, time, reason for creation and creator.
- (c) Prompt the creator of an extract to assign it to a folder at a level specified by the Administrator at configuration time.
- (d) Store a cross-reference to an extract in the same folder and volume as the original record, even if that volume is closed.
- (e) Store changes made in the redacting process in the audit trail.
- (f) Provide functionality for redacting sensitive information from an extract record or support this being done by another software package. Ensure that 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.

ACCEPTANCE OF TERMS AND CONDITIONS

Please indicate your acceptance of the terms and conditions relating to this EOI document.

Accepted for and on behalf of:

Vendor Name:

Name:

Position:

Date: