



Ministry of Management Services

Request for Proposal

Enterprise Document and Records Management System

Request for Proposal No. <<>>

Issue date:

Date: October 16, 2001

Closing location:

Purchasing Commission
P.O. Box 9476, Stn. Prov. Gov't.
3350 Douglas Street, Suite 102
Victoria, B.C. V8W 9W6
Attention: David Simon
Telephone: (250) 387-7326
Facsimile: (250) 387-7310

Email: David.M.Simon@gems9.gov.bc.ca

Closing date and time:

Ten (10) bound copies of the complete proposal, along with one electronic copy must be received by 2:00 PM Pacific Time on November 26, 2001

Date and location of Proponents' meeting:

Date and Time: 2:00 p.m. - October 26, 2001
Street Address: Ocean Point Resort, Balfour Room
45 Songhees Road
City: Victoria, B.C.

Attendance at the Proponents' meeting is not mandatory

This page is intentionally left blank

Table of Contents

EXECUTIVE SUMMARY	5
1 SUMMARY OF THE REQUIREMENT	5
ADMINISTRATIVE REQUIREMENTS	7
2 REQUEST FOR PROPOSAL TERMINOLOGY	7
3 REQUEST FOR PROPOSAL PROCESS.....	7
3.1 <i>Receipt Confirmation Form</i>	7
3.2 <i>Enquiries</i>	7
3.3 <i>Proponents' Meeting</i>	8
3.4 <i>Closing Date</i>	8
3.5 <i>Late Proposals</i>	8
3.6 <i>Eligibility</i>	8
3.7 <i>Evaluation Committee</i>	9
3.8 <i>Evaluation and Selection</i>	9
3.9 <i>Negotiation Delay</i>	9
3.10 <i>Debriefing</i>	9
3.11 <i>Estimated Time-Frames</i>	9
4 PROPOSAL PREPARATION	10
4.1 <i>Signed Proposals</i>	10
4.2 <i>Alternative Solutions</i>	10
4.3 <i>Irrevocability of Proposals</i>	10
4.4 <i>Changes to Proposal Wording</i>	10
4.5 <i>Working Language of the Province</i>	10
4.6 <i>Proponents' Expenses</i>	10
4.7 <i>Limitation of Damages</i>	10
4.8 <i>Proposal Validity</i>	11
4.9 <i>Firm Pricing</i>	11
4.10 <i>Currency and Taxes</i>	11
4.11 <i>Completeness of Proposal</i>	11
5 ADDITIONAL TERMS.....	11
5.1 <i>Sub-Contracting</i>	11
5.2 <i>Acceptance of Proposals</i>	12
5.3 <i>Definition of Contract</i>	12
5.4 <i>Form of Contract</i>	12
5.5 <i>Liability for Errors</i>	12
5.6 <i>Modification of Terms</i>	12
5.7 <i>Ownership of Proposal</i>	12
5.8 <i>Use of Request for Proposal</i>	12
5.9 <i>Confidentiality of Information</i>	13
5.10 <i>Reciprocity</i>	13
PROJECT REQUIREMENTS	14
6 MINISTRY/SITUATION OVERVIEW	14
6.1 <i>Ministry Responsibilities</i>	14
6.1.1 Ministry of Management Services	14
6.1.2 British Columbia Archives	14
6.1.3 Other Ministries, Crown Corporations, Agencies	15
6.2 <i>Background</i>	15
6.3 <i>Legislation, Policies and Standards</i>	16
6.3.1 Document Disposal Act	17
6.3.2 Freedom of Information (FOI) and Protection of Privacy Act (FOIPPA).....	17
6.3.3 Other Legislation	18

6.3.4	Government Management Operating Policy (GMOP) and Financial Administration Operating Policy (FAOP).....	18
6.3.5	Administrative Records Classification System (ARCS) and Operational Records Classification Systems (ORCS).....	18
6.4	Other Government Initiatives	20
6.5	Other Considerations.....	21
7	REQUIREMENTS AND PROJECT SCOPE	21
7.1	Project Scope, Budget and Timeframes	21
7.1.1	Project Scope	21
7.1.2	Basic Requirements	23
7.1.3	Key Deliverables	25
7.1.4	Budget.....	26
7.1.5	Timing	26
7.1.6	Out of Scope	26
8	EVALUATION CRITERIA.....	27
8.1	Mandatory.....	27
8.2	Desirable.....	28
9	PROONENT RESPONSE.....	29
9.1	To Meet Mandatory Criteria.....	29
9.2	To Meet Desirable Criteria.....	29
10	PROPOSAL FORMAT.....	30
APPENDICES.....		31
APPENDIX A PROPOSAL COVERING LETTER		32
APPENDIX B FORM OF CONTRACT		33
APPENDIX C PROONENT CHECKLIST.....		35
APPENDIX D RECEIPT CONFIRMATION FORM		36
APPENDIX E HIGH LEVEL REQUIREMENTS (RECORDS MANAGEMENT)		37
APPENDIX F DESIRABLE SYSTEM REQUIREMENTS.....		49
APPENDIX G DRAFT META-DATA ELEMENTS.....		99
APPENDIX H ARCS/ORCS MASTER DATABASE.....		106
APPENDIX I TECHNOLOGY INFRASTRUCTURE.....		110

Executive Summary

1 Summary of the Requirement

The British Columbia government is seeking proposals from qualified Proponents to provide an Enterprise Document and Records Management System (EDRMS) that consists of an integrated records management and document management tool set. The government expects to select one or more software tools to be made available on all desktops within BC government ministries, agencies and crown corporations. The Province intends that the EDRMS selected through this RFP will become the Province's standard EDRMS software. As a result of this initiative, all employees will have the ability to manage electronic and physical documents and records in a consistent manner from their desktops.

The government of British Columbia wishes to significantly improve its capability to manage the documents and records in its possession. A key objective is to establish an infrastructure for effectively managing all BC government records -- i.e., an infrastructure that builds upon existing standards and processes for managing physical records and incorporates requirements for electronic documents and records. A critical step to being able to do this is the selection of appropriate software that can be made available on all desktops.

The vision of the government is that:

The BC government will be able to effectively manage all of its documents and records in a consistent, logical manner, from creation to final disposition, using a common set of tools, standards and policies.

This RFP focuses on Records Management (RM) functional requirements. Nevertheless, there is a strong interest within government to have an application infrastructure upon which other document-centric applications can be built. The key objective of this RFP is to provide an Enterprise Document and Records Management System (EDRMS) that can be used across government. The requirements section of this RFP draws heavily on the Model Requirements for Electronic Records management developed for the European Community. (MoReq). The BC government has a need for a system that is robust and scalable -- the system will ultimately be deployed to all government desktops to provide a unified tool set for managing electronic and physical records. There are currently just under 34,000 desktops in government, but proposed restructuring may result in a lower number of software installations. For the purpose of evaluating this RFP, 30,000 desktops will be the estimated number of desktops on which the software may be installed. The actual number may be less.

The initial priority of government is to manage its electronic documents and records, beginning with those created in the Microsoft Outlook and Microsoft Office suite of products. The EDRMS selected will also be expected to handle other types of files as the

product use is extended. These would include CAD and other drawings, maps, photographs, scanned images, sound and movie formats, web pages as well as physical documents. Any solution adopted as a result of this RFP will have to work within the BC government technical environment and may need to integrate with existing government systems. The EDRMS chosen for government will be required to schedule records using the government standard system for classification, retention and disposition, including the *Administrative Records Classification System (ARCS)*, *Operational Records Classification Systems (ORCS)* and other approved records schedules. BC Archives may construct an Oracle database to store final versions of *ARCS* and *ORCS* as well as information on the development and history of the final approved version. The EDRMS should be able to use this database as the reference or source for file numbers in the records management component of the EDRMS.

The central licence custodian will be the Information Technology Services Division (ITSD) of the Ministry of Management Services.

Administrative Requirements

The following terms will apply to this Request for Proposal and any subsequent Contract. The submission of a proposal in response to this Request indicates acceptance of all the following terms.

2 Request for Proposal Terminology

Throughout this Request for Proposal, terminology is used as follows:

“Contract” means the written agreement resulting from this Request for Proposal executed by the Province and the Contractor;

“Contractor” means the successful Proponent to this Request for Proposal who enters into a written Contract with the Province;

“Ministry” means Ministry of Management Services;

“Must” or “mandatory” means a requirement that must be met in order for a proposal to receive consideration;

“Proponent” means an individual or a company that submits, or intends to submit, a proposal in response to this “Request for Proposal”;

“Province” means Her Majesty the Queen in Right of the Province of British Columbia and includes the Purchasing Commission and the Ministry;

“Purchasing Commission” means the Purchasing Commission pursuant to the Purchasing Commission Act, RSBC 1996, Chapter 392;

“Should” or “desirable” means a requirement having a significant degree of importance to the objectives of the Request for Proposal.

3 Request for Proposal Process

3.1 Receipt Confirmation Form

Proponents are advised to fill out and return the attached Receipt Confirmation Form. All subsequent information regarding this Request for Proposal, including changes made to this document will be directed only to those Proponents who return the form. Subsequent information will be distributed by the method authorized on the Receipt Confirmation Form Shown in **Appendix D**.

3.2 Enquiries

All enquiries related to this Request for Proposal are to be directed, in writing, to the following person. Information obtained from any other source is not official and must not be relied upon. Enquiries and responses will be recorded and may be distributed to all Proponents at the Province’s option. Questions received after the Proponent’s meeting will be answered if time permits. Include the Request for Proposal Number and Title in all correspondence.

Purchasing Commission
P.O. Box 9476, Stn. Prov. Gov't.
3350 Douglas Street, Suite 102
Victoria, B.C. V8W 9W6
Attention: David Simon
Fax: (250) 387-7310
E-mail: David.M.Simon@gems9.gov.bc.ca

3.3 Proponents' Meeting

A Proponents' meeting will be held at the time and in the location specified on the front page of this Request for Proposal. A transcript or minutes of the meeting will be distributed to those Proponents who have returned the Receipt Confirmation Form. Attendance is optional. Oral questions will be allowed at the Proponents' meeting. However, questions of a complex nature, or questions where the Proponent requires anonymity, must be forwarded in writing, prior to the meeting, to the person designated above.

3.4 Closing Date

Ten (10) bound copies of the complete proposal, along with one electronic copy, must be received by 2:00 PM, Pacific Time, on November 26, 2001 at:

Purchasing Commission
P.O. Box 9476, Stn Prov Gov't
3350 Douglas Street, Suite 102
Victoria, B.C. V8W 9W6
Attention: David Simon
Telephone: (250) 387-7326
Facsimile: (250) 387-7310
Email: David.M.Simon@gems9.gov.bc.ca

Proposals must not be sent by facsimile. Proposals and their envelopes must be clearly marked with the name and address of the Proponent, the Request for Proposal number, and the project or program title.

3.5 Late Proposals

Late proposals will not be accepted and will be returned to the Proponent.

3.6 Eligibility

Proposals will not be evaluated if the Proponent's current or past corporate or other interests may, in the Province's opinion, give rise to a conflict of interest in connection with this project.

The provincial government contracted EDS Canada to provide assistance in preparing this RFP. Their role was to organize a large amount of material that had already been gathered by the province into the RFP format. They did not conduct any user requirements interviews. EDS prepared a working draft of the RFP, which was then finalized by the

province. EDS had no input to the evaluation criteria or the weighting of the various evaluation factors. EDS will be eligible to submit a response to this RFP.

Proposals from not-for-profit agencies will be evaluated against the same criteria as those received from any other Proponents.

3.7 Evaluation Committee

Evaluation of proposals will be by a committee formed by the Province and may include a representative of the Purchasing Commission or other government ministry.

3.8 Evaluation and Selection

The evaluation committee will check proposals against the mandatory criteria. Proposals not meeting all mandatory criteria will be rejected without further consideration. Proposals that do meet all the mandatory criteria will then be assessed and scored against the desirable criteria. The Province's intent is to enter into a Contract with the Proponent who has the highest overall ranking.

The ministry may generate a short list of Proponents from scores realised in their RFP responses. These Proponents may be requested to provide further details on their approach and costing. They may also be asked to demonstrate their elements of their response through interactive demonstrations involving specific scenarios and hands-on evaluation by a ministry team.

3.9 Negotiation Delay

If a written Contract cannot be negotiated within thirty days of notification of the successful Proponent, the Province may, at its sole discretion at any time thereafter, terminate negotiations with that Proponent and either negotiate a Contract with the next qualified Proponent or choose to terminate the Request for Proposal process and not enter into a Contract with any of the Proponents.

3.10 Debriefing

At the conclusion of the Request for Proposal process, all Proponents will be notified. Unsuccessful Proponents may request a debriefing meeting with the Province.

3.11 Estimated Time-Frames

The following timetable outlines the anticipated schedule for the Request for Proposal and Contract process. The timing and the sequence of events resulting from this Request for Proposal may vary and shall ultimately be determined by the Province.

Event	Anticipated Date
Request for Proposal is issued	October 16, 2001
Proponents' meeting	October 26, 2001
Request for Proposal closes	November 26, 2001
Proponent short list announced	December 7, 2001
Short list demonstrations completed (if required)	December 19, 2001

Successful Proponent announced	December 21, 2001
Contract is signed	January 30, 2002

4 Proposal Preparation

4.1 Signed Proposals

A person authorised to sign on behalf of the Proponent and to bind the Proponent to statements made in response to this RFP must sign the proposal. The proposal must include a letter or statement(s) substantially similar in content to the sample Proposal Covering Letter provided in **Appendix A**.

4.2 Alternative Solutions

If alternative solutions are offered, please submit the information in the same format, as a separate proposal.

4.3 Irrevocability of Proposals

By submission of a clear and detailed written notice, the Proponent may amend or withdraw its proposal prior to the closing date and time. Upon closing time, all proposals become irrevocable. By submission of a proposal, the Proponent agrees that should its proposal be successful the Proponent will enter into a Contract with the Province.

4.4 Changes to Proposal Wording

The Proponent will not change the wording of its proposal after closing and no words or comments will be added to the proposal unless requested by the Province for purposes of clarification.

4.5 Working Language of the Province

The working language of the Province of British Columbia is English and all responses to this Request for Proposal must be in English.

4.6 Proponents' Expenses

Proponents are solely responsible for their own expenses in preparing a proposal and for subsequent negotiations with the Province, if any. If the Province elects to reject all proposals, the Province will not be liable to any Proponent for any claims, whether for costs or damages incurred by the Proponent in preparing the proposal, loss of anticipated profit in connection with any final Contract, or any other matter whatsoever.

4.7 Limitation of Damages

Further to the preceding paragraph, the Proponent, by submitting a proposal, agrees that it will not claim damages, for whatever reason, relating to the Contract or in respect of the competitive process, in excess of an amount equivalent to the reasonable costs incurred by the Proponent in preparing its proposal and the Proponent, by

submitting a proposal, waives any claim for loss of profits if no agreement is made with the Proponent.

4.8 Proposal Validity

Proposals will be open for acceptance for at least 90 days after the closing date.

4.9 Firm Pricing

Prices will be firm for the entire Contract period unless this Request for Proposal specifically states otherwise.

4.10 Currency and Taxes

Prices quoted are to be:

In Canadian dollars;

Inclusive of duty, where applicable;

FOB destination, delivery charges included where applicable; and

Exclusive of Goods and Services Tax and Provincial Sales Tax.

4.11 Completeness of Proposal

By submission of a proposal the Proponent warrants that, if this Request for Proposal is to design, create or provide a system or manage a program, all components required to run the system or manage the program have been identified in the proposal or will be provided by the Contractor at no charge.

5 Additional Terms

5.1 Sub-Contracting

- a) Using a sub-contractor (who must be clearly identified in the proposal) is acceptable. This includes a joint submission by two Proponents having no formal corporate links. However, in this case, one of these Proponents must be prepared to take overall responsibility for successful performance of the Contract and this must be clearly defined in the proposal.
- b) Sub-contracting to any firm or individual whose current or past corporate or other interests may, in the Province's opinion, give rise to a conflict of interest in connection with this project will not be permitted. This includes, but is not limited to, any firm or individual involved in the preparation of this Request for Proposal.
- c) Where applicable, the names of approved sub-contractors listed in the proposal will be included in the Contract. No additional subcontractors will be added, nor other changes made, to this list in the Contract without the written consent of the Province.

5.2 Acceptance of Proposals

This Request for Proposal must not be construed as an agreement to purchase goods or services. The Province is not bound to enter into a Contract with the Proponent who submits the lowest priced proposal or with any Proponent. Proposals will be assessed in light of the evaluation criteria. The Province will be under no obligation to receive further information, whether written or oral, from any Proponent.

Neither acceptance of a proposal nor execution of a Contract will constitute approval of any activity or development contemplated in any proposal that requires any approval, permit or license pursuant to any federal, provincial, regional district or municipal statute, regulation or by-law.

5.3 Definition of Contract

Notice in writing to a Proponent that it has been identified as the successful Proponent and the subsequent full execution of a written Contract will constitute a Contract for the goods or services, and no Proponent will acquire any legal or equitable rights or privileges relative to the goods or services until the occurrence of both such events.

5.4 Form of Contract

By submission of a proposal, the Proponent agrees that, should it be identified as the successful Proponent, it is willing to enter into a Contract with the Province in accordance with the terms set out in **Appendix B**.

5.5 Liability for Errors

While the Province has used considerable efforts to ensure an accurate representation of information in this Request for Proposal, the information contained in this Request for Proposal is supplied solely as a guideline for Proponents. The information is not guaranteed or warranted to be accurate by the Province, nor is it necessarily comprehensive or exhaustive. Nothing in this Request for Proposal is intended to relieve Proponents from forming their own opinions and conclusions with respect to the matters addressed in this Request for Proposal.

5.6 Modification of Terms

The Province reserves the right to modify the terms of this Request for Proposal at any time in its sole discretion. This includes the right to cancel this Request for Proposal at any time prior to entering into a Contract with the successful Proponent.

5.7 Ownership of Proposal

All documents, including proposals, submitted to the Province become the property of the Province. They will be received and held in confidence by the Province, subject to the provisions of the Freedom of Information and Protection of Privacy Act.

5.8 Use of Request for Proposal

This document or any portion thereof, may not be used for any purpose other than the submission of proposals.

5.9 Confidentiality of Information

Information pertaining to the Province obtained by the Proponent as a result of participation in this project is confidential and must not be disclosed without written authorization from the Province.

5.10 Reciprocity

The Province may consider and evaluate any proposals from other jurisdictions on the same basis that the government purchasing authorities in those jurisdictions would treat a similar proposal from a British Columbia supplier.

Project Requirements

6 Ministry/Situation Overview

The Ministry of Management Services, on behalf of the BC government, is issuing this RFP. BC Archives is an organisational unit within the Ministry of Management Services. The Project Director reports to the Provincial Archivist.

BC Archives is the central agency responsible for the management of information, documents and records across government. It has become clear that the government must manage its electronic records more effectively and consistently than it has to date. Government believes the technology and the software tools available to do this are now at a stage to enable integrated document/record management both within individual ministries and across organisations.

6.1 Ministry Responsibilities

6.1.1 Ministry of Management Services

The Ministry of Management Services is responsible for the provision and overall management of shared government services. The Ministry is committed to bringing accountability, fair treatment, competition and sound fiscal management to the way government delivers its shared services within the government and to the public.

Responsibilities include:

- Developing and implementing information technology standards and policies consistent with the IT strategies developed by the CIO for government;
- Providing common IT infrastructure and services;
- Sponsoring strategic IT initiatives which cross ministry or agency boundaries and require strong central management;
- Developing, integrating and implementing government standards and policies related to management of records and information;
- Preserving the documentary heritage of the province;
- Ensuring there is appropriate access to government information;
- Ensuring personal and private information held by government is properly protected.

6.1.2 British Columbia Archives

BC Archives is the central archives service for the government of British Columbia, and provides research access to records of enduring value to the province for both the provincial government and public clientele. BC Archives is also the central agency responsible for information and records management within the provincial government.

Responsibilities for records management include:

- Providing central direction and control to organizations within the BC government for records management programs;
- Providing a variety of services to assist ministries and other clients to systematically manage the creation, use, access, retention, disposal, and preservation of government's recorded information in all forms;
- Establishing standards and maintaining a policy framework to ensure the accountability of ministries for the management of their information and records;
- Advising and assisting ministries in maintaining efficient information management, imaging and micrographic systems and establishing life-cycle schedules for both administrative and operational records;
- Providing cost-effective storage, retrieval and disposal services for ministries' semi-active and inactive records.

6.1.3 Other Ministries, Crown Corporations, Agencies

Ministries, Crown Corporations and Agencies are responsible for the administration, control, documentation, access, preservation and security of records in their custody and control.

Responsibilities for records management include:

- Designating a full time Ministry Records Officer or equivalent whose major responsibility is to administer the recorded information management program;
- Creating or acquiring records to sufficiently document organizational activity and meet administrative, legal, evidential and accountability requirements;
- Preserving and protecting records by establishing and implementing appropriate procedures for their security, handling, use and storage;
- Maintaining, controlling and documenting their records in a manner that permits efficient access and retrieval;
- Scheduling all records using standard systems for classification, retention and disposition, including the *Administrative Records Classification System (ARCS)*, *Operational Records Classification System (ORCS)*, and other approved records schedules.

6.2 Background

The government of British Columbia intends to significantly increase its capability to manage the documents and records in its possession. A key objective is to establish an infrastructure for effectively managing all BC government records -- i.e., an infrastructure that builds upon existing standards and processes for managing physical records and incorporates requirements for electronic documents and records. A critical step to being able to do this is the selection of appropriate software that can be made

available on all desktops. As a result of this initiative, all government employees will have the policies, standards and necessary tools to manage physical and electronic documents and records in a consistent manner from their desktops.

An initial review of document management and records management software has resulted in a conclusion that there are few, if any, single software packages that have the range of functionality that is desired. Government is therefore prepared to accept a suite of software tools that can operate together in a seamless way to provide Enterprise Document and Records Management functionality. While there is a strong desire to purchase commercial off-the-shelf software, there is a recognition that there may be a need for some level of custom integration within the suite of software proposed, or to ensure that the software links easily to other applications and systems currently in use in the BC government. Extensive customisation is not desired.

High level business requirements for the Records Management component have been developed by a working group of Ministry Records Officers. These were informed by the current BC government procedures for managing physical records and anticipated needs for management of electronic records. These requirements are presented in **Appendix E** for information.

Ministry officials have reviewed a number of Electronic Records Management systems requirements documents from other jurisdictions and have identified key systems requirements along with additional needs specific to the BC government, based on the defined business requirements. The systems requirements are found in **Appendix F**.

The requirements have drawn heavily on the European Community Model Requirements for the Management of Electronic Records (MoReq). The full MoReq can be found at <http://www.cornwell.co.uk/moreq>.

For the baseline requirements for management of electronic records, government will rely on the United States Department of Defence standard baseline set of functions for Records Management Application (RMA) software (DoD 5015.2-STD). Any records management software certified to meet this standard would meet the baseline requirements for the electronic records management component of this RFP. The US National Archives and Records Administration (NARA) has endorsed use of DoD 5015.2-STD as a standard for Records Management within the United States government. As result, DoD 5015.2-STD has attracted a wide interest beyond the DoD and is increasingly used as the baseline for electronic records management software. More information can be found at <http://jtc.fhu.disa.mil/recmgt>.

6.3 Legislation, Policies and Standards

The government of British Columbia has specific business rules for managing its information resources. They come in the form of authorities such as: legislation, regulations, policies (*Government Management Operating Policy (GMOP)*), (*Financial Administration Operating Policy (FAOP)*), and standards (records classification and scheduling systems (ARCS/ORCS)). Any software proposed for the management of documents and records should operate within this legislative and policy framework. The following subsections provide additional background for respondents on the information

management requirements and authorities governing the creation and management of government's electronic records.

Once the software has been selected, BC Archives intends to review the policies and standards to determine what, if any, changes should be made to maximise the likelihood of successful implementation of the selected software.

6.3.1 Document Disposal Act

The Public Documents Committee supervises the retention and disposal of government documents. The storage and disposal obligations for recorded information are set out in the *Document Disposal Act* (RSBC 1996 c. 99). This statute sets out the approval process for the disposal, through transfer to the British Columbia Archives or destruction, of all government recorded information, including documents and records. For more information see the http://www.qp.gov.bc.ca/statreg/stat/D/96099_01.htm.

The *Document Disposal Act* defines approval requirements for the retention and disposition of records and recorded information. The *Administrative Records Classification System* (ARCS) and *Operational Records Classification Systems* (ORCS) are approved under the provisions of the *Document Disposal Act* and describe types of administrative and operational records and specify their retention periods. The *Document Disposal Act* establishes procedures for the approval of the records schedules and classification systems developed by the BC Archives and government ministries.

ARCS was developed by the BC Archives and approved by the Public Documents Committee and the Select Standing Committee on Public Accounts (commonly called the Public Accounts Committee). It was then approved by resolution of the Legislative Assembly in 1987. That resolution established ARCS as the retention and disposition schedule for the administrative records of the government of British Columbia. For more information on the Public Documents Committee, see <http://www.bcarchives.gov.bc.ca/infomgmt/committe/pdc>.

Operational records relate to the operations and services provided by a ministry or agency in carrying out the functions for which it is responsible according to statute, mandate, or policy. Each ORCS is tailored to fit the specific operational records of a unit of government. BC Archives establishes standards for the development of ORCS for all operational records of the government of British Columbia. For more information refer to the http://www.bcarchives.gov.bc.ca/infomgmt/policy/policy.htm#std_orcs_kit.

6.3.2 Freedom of Information (FOI) and Protection of Privacy Act (FOIPPA)

The *Freedom of Information and Protection of Privacy Act* (RSBC 1996, c. 165) governs access to and privacy protection for all BC government records. For more information see: http://www.qp.gov.bc.ca/statreg/stat/F/96165_01.htm.

The purpose of the *Freedom of Information and Protection of Privacy Act* is to make public bodies more accountable to the public and to protect personal privacy by:

- Giving the public a right of access to records;
- Giving individuals a right of access to, and a right to request correction of, personal information about themselves;
- Specifying limited exceptions to the rights of access;
- Preventing the unauthorized collection, use or disclosure of personal information by public bodies;
- Providing for an independent review of decisions made under this Act.

6.3.3 Other Legislation

Additional legislation that can affect the management of records within the BC government includes:

- The *Interpretation Act* (RSBC 1996, c. 238) establishes definitions that must apply to the interpretation of information and practice of Records Management in British Columbia. For more information see http://www.qp.gov.bc.ca/statreg/stat/I/96238_01.htm;
- The *Business Paper Reduction Act* (SBC 1998, c. 26) facilitates streamlining of the ways that businesses deal with the Provincial and local governments. For more information see http://www.qp.gov.bc.ca/statreg/stat/B/98026_01.htm;
- *Electronic Transactions Act* (Bill 13, 2001) establishes that electronic documents and electronic signatures are as valid as their paper equivalents. For more information see http://www.legis.gov.bc.ca/2001/3rd_read/gov13-3.htm.

6.3.4 Government Management Operating Policy (GMOP) and Financial Administration Operating Policy (FAOP)

Responsibility for managing government records is established by Treasury Board policy and described in the *General Management Operating Policy (GMOP) and Financial Administration Operating Policy (FAOP)* manuals. See <http://www.fin.gov.bc.ca/ocg/fmb/manuals/manuals.htm>.

Government-Wide Records Management policy is published in this *Government Management Operating Policy (GMOP)* [chapter 8.3.2], which specifies the responsibilities of ministries and BC Archives' responsibility for establishing standards. Revision of *GMOP* involves a consultative process with the ministries. Ministry Records Officers (MRO's) are the primary links between the ministries and BC Archives. See *Government Management Operating Policy* (chapter 8.3.2) <http://www.fin.gov.bc.ca/ocg/fmb/manuals/gmop/gm8.html>.

6.3.5 Administrative Records Classification System (ARCS) and Operational Records Classification Systems (ORCS).

Records classification and scheduling for all government ministries follow the *Administrative Records Classification System (ARCS)* and the program-specific

Operational Records Classification Systems (ORCS). These systems establish classes of records and define retention periods and final dispositions for records in the classes. *ARCS* and *ORCS* are the definitive sources for records management file numbers. They are the mechanisms approved in the *Document Disposal Act* for classifying records in accordance with a standard administrative and operational records typology and for establishing records retention and disposition requirements. For more information on *ARCS*, *ORCS* and Special Records Schedules see *ARCS Online* at <http://www.bcarchives.gov.bc.ca/arcs/index.htm>.

ARCS/ORCS make up a comprehensive management plan for all government records and tools for executive control of recorded information. Administrative records are common to all ministries and pertain to "housekeeping" functions (finance, personnel, equipment and supplies, facilities, computer systems, and general administration). Operational records are specific to the mandate, role, or activity of a ministry or agency and consequently differ in content, but not structure, from organisation to organisation.

ARCS/ORCS integrate a number of vital information management concepts for the records of the government of British Columbia, regardless of physical format/media. *ARCS/ORCS* is:

- A filing and classification system - *ARCS/ORCS* facilitate access and retrieval in the office;
- A records retention and disposal schedule - *ARCS/ORCS* provide a legal basis for the integrity, authenticity, and completeness of government's records, as well as ongoing authority for the management of those records;
- A framework for the audit and review of administrative/operational functions - *ARCS/ORCS* also provide a framework to streamline disposal of routine records and duplicate and protect records with long-term values.

The following details how the BC government uses *ARCS/ORCS*:

- Information that has been created, collected, maintained and/or retained by a government agency must be classified and scheduled within *ARCS* or that agency's *ORCS*, regardless of its media;
- Electronic records are to be retained in accordance with approved records schedules. The current legal custodian ensures that the records are appropriately maintained and are accessible until the point of final disposition;
- Records scheduled for destruction are to be destroyed in accordance with approved government policy and procedures. Records scheduled for archival retention will be maintained by the current legal custodian until transfer to the legal custody of BC Archives;
- An *ORCS* is not complete unless the information flow of an agency's computer system(s) is/are analyzed and the records created, stored and generated by the system(s) is/are scheduled;
- The additional technological information required for the scheduling of operational electronic records is documented in the Information System Overview (ISO) formats used for *ORCS*;

- Electronic mail sent or received by government equipment is a government record;
- Attachments to electronic messages (including electronic attachments, transmission history, etc.) are an integral part of electronic mail;
- Electronic mail is subject to the same management controls as other government records including the disposition requirements of the *Document Disposal Act* and the retention periods in approved records schedules (including the special schedules published in *ARCS*. Information held in government electronic mail systems may be subject to a request for information under the *Freedom of Information and Protection of Privacy Act*;
- An ongoing records schedule is a short-term, temporary solution to ongoing records disposition problems. It represents an analysis of one or more organized records series, of either administrative or operational records, but does not reflect an analysis of the records within their larger information system context. Such schedules authorize, on a continuing basis, final disposition of the records described within the scheduling document;
- Upon approval of an *ORCS*, ongoing records schedules which previously applied to records covered by the *ORCS* are superseded, except in cases where the ongoing records schedule contains a sunset clause or covers a defunct record series in the operational area covered by an *ORCS*;
- Some categories of records or data have special retention and disposition requirements and may be handled by developing special records schedules. These schedules can be standardized for all ministries, and can cover both administrative and operational records. They can be used effectively to dispose of routine records and ephemeral material, can be adjusted to meet the retention problems posed by changing technologies, and can protect the long-term values of executive records.

For the full ministry records management policy, including the Recorded Information Management Manual see <http://www.bcarchives.gov.bc.ca/infomgmt/policy/policy.htm>.

6.4 Other Government Initiatives

The Province of British Columbia is developing eGovernment strategies under an initiative formerly known as InfoSmart. To implement this effectively, the government must be able to manage records generated from electronic service delivery and e-commerce applications in a consistent and cost-effective manner that complies with all BC government information management standards. Proponents will find detailed information on this initiative at http://www.cio.gov.bc.ca/Strategic_Initiatives/eGov.htm.

The British Columbia government is also in the process of issuing a Request for Proposal for an Enterprise-Wide Government Portal. Although there is no overlap between these two projects, Proponents may wish to review the Portal RFP as it relates

to EDRMS and content management requirements and its linkage to other government initiatives.

6.5 Other Considerations

The central license custodian will be the Information Technology Services Division (ITSD) of the Ministry of Management Services.

7 Requirements and Project Scope

The BC government has a good set of policies and procedures in place and there are existing software packages being used to deal with physical records. The project will allow ministries to more effectively manage electronic records and documents in an integrated manner in compliance with IM legislation and policies.

This project will provide the government with an Enterprise Document and Records Management System (EDRMS) that will consist of an integrated set of software tools for records management and document management. This section outlines and describes the general requirements the government has for an EDRMS. The specific requirements that Proponents will be evaluated on are described in Section 8 and **Appendix F**.

This RFP may result in two contractual relationships, one with the BC government generally and one with the BC Assessment Authority.

7.1 Project Scope, Budget and Timeframes

7.1.1 Project Scope

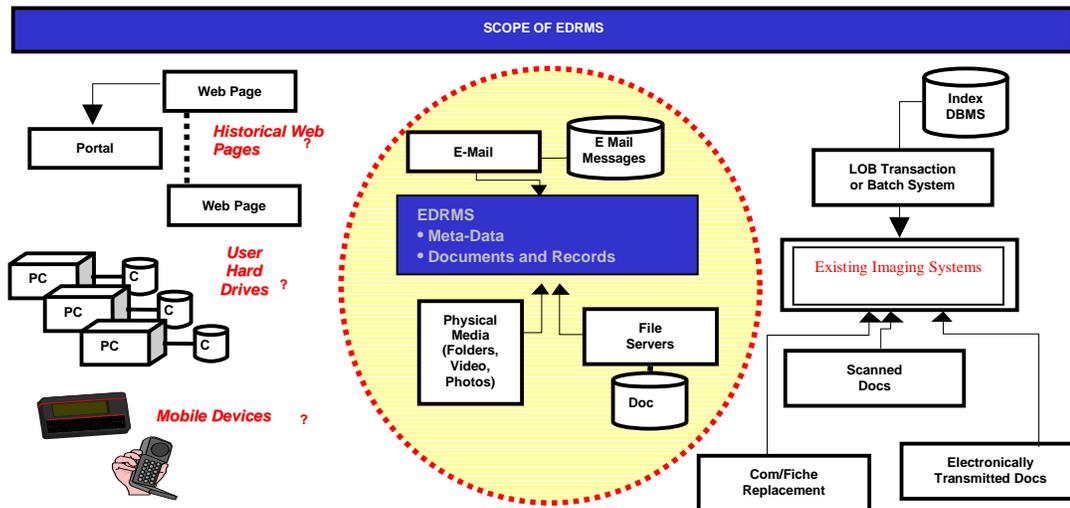
Government will select one or more software tools that can be installed on all desktops within government ministries, agencies and crown corporations. As a result of this initiative, all employees will have the ability to manage all forms of documents and records regardless of location, media or file type in a consistent manner from their desktops.

This software selected will be expected to handle electronic and physical records with equal facility. The software must be robust, scalable and flexible in its configuration and its ability to pass information to other software being used in records management or in lines of business within a ministry.

The vision that is trying to be achieved can be stated as follows:

The BC government will be able to effectively manage all of its documents and records in a consistent, logical manner, from creation to final disposition, using a common set of tools, standards and policies.

Figure 1 is a high-level schematic showing the general scope of the EDRMS project. The priority issues are contained within the circle. Most of the elements outside the circle are lower priority issues that will be incorporated over time.



Any scanning, OCR and/or electronic transmission of documents that are inherent in a ministry business process are out of scope of this RFP, but the records created in or from those processes must be able to be managed by the EDRMS selected.

From an imaging functionality point of view, the system must be able to import images, and indexing/metadata created from other imaging systems and capture applications, and then offer a standard document management interface. It should also offer a development environment capable of creating dedicated LOB imaging applications (custom application) integrating all of the document and records management functionality and technologies (including storage management, index/metadata management, image processing/conversion, redaction, OCR, and COLD).

The initial priority for government is to use the EDRMS software to manage common forms of electronic records and all forms of physical (hardcopy) records. For electronic records, this includes documents generated from the Microsoft Office Suite and e-mail. Although this initial priority deals with a limited numbers of document formats, the EDRMS will be expected to handle virtually all types of electronic documents used in government. These include, but are not limited to electronic forms, CAD, other drawing and image formats, maps, photographs, scanned images, audio and video clips.

Once the software is installed, there will be subsequent opportunities for ministries to review their business processes to take fuller advantages of the capabilities in the EDRMS suite. There may also be opportunities to replace existing stand-alone systems that perform functions within the software chosen.

Any solution adopted for an EDRMS will have to operate within the BC government technical environment and potentially pass information or receive information to/from a wide variety of other programs. Several electronic service delivery, e-commerce and business-focused document/content management initiatives are proposed or underway across government which will be creating new and additional records. It will be important that the software chosen can easily deal with these developments, by simple configuration choices and/or open access, standard APIs, etc.

Government records are managed with a file classification system that uses block-numeric file numbers that have associated retention schedules and other information (*ARCS/ORCS*). The EDRMS chosen for government should be able to use *ARCS/ORCS* data without the need to manually enter existing schedules. Depending on the way in which the records management portions of the software does this, BC Archives may construct an Oracle database to store final versions of *ARCS* and *ORCS* as well as information on the development and history of the approval process. The EDRMS should be able to use such a database as a reference or source for file numbers and retention information or hold such information for use by the EDRMS and other systems. A description of the *ARCS/ORCS* database elements is in **Appendix H**. The detailed requirements and system design for an *ARCS/ORCS* database has been completed but may need to reflect the capabilities of the EDRMS solution selected.

7.1.2 Basic Requirements

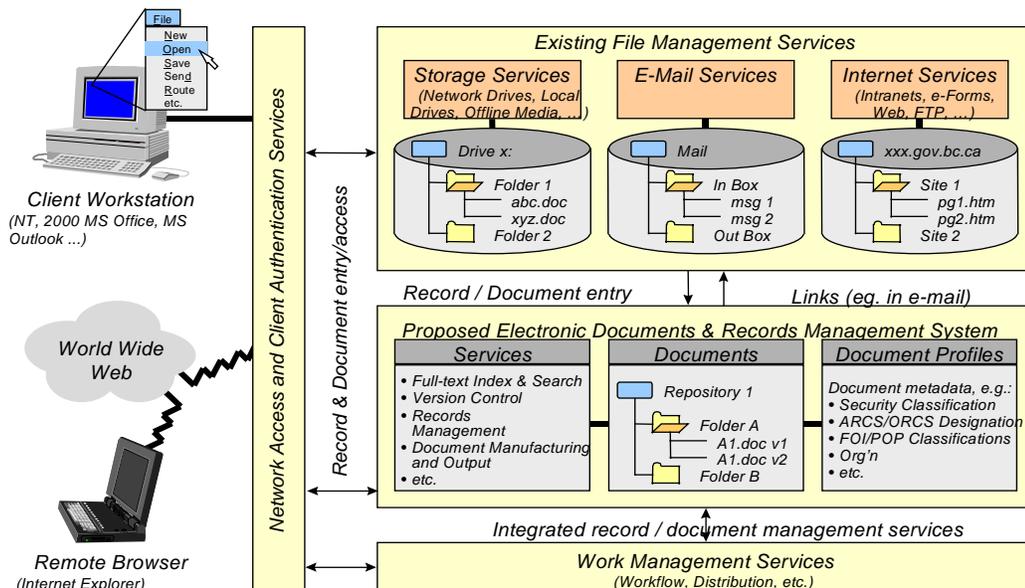
The basic requirement is for an integrated records management and document management tool set to be available on all desktops within BC government ministries, agencies and crown corporations. This will provide the ability for all employees to directly manage electronic documents and records stored in multiple repositories in a variety of file types in a consistent manner from their desktops.

For each organisation (e.g., ministry/program), the EDRMS should support integrated management of all office records; i.e., all office e-records (WP, email, spreadsheets, presentations etc) and all types of physical records. The EDRMS should also be extensible in future to cover other document types (images, database reports, voicemail, etc).

The EDRMS should be able to store, retrieve and view files in their native format without a need to have the applications that generated the file present.

The integrated records and document management system should be incorporated as seamlessly as possible into the BC government system infrastructure. Figure 2 is a conceptual illustration of what this means.

Figure 2



Scaling and Robustness

The EDRMS should be built on a robust, scalable architecture supporting such requirements as:

- EDRMS application(s) on every employee desktop (30,000+ users);
- Multiple, large shared record and document repositories across multiple platforms;
- All components of the solution must be equally scalable and robust.

The following estimates indicate the volume of information produced per year by the BC government, which must be managed by the EDRMS:

- 50,000,000 E-Mail Messages: 5,000,000 with attachments;
- 15,000,000 MS Office Documents;
- 2,000,000 physical volumes (e.g., file folders), comprising approximately 30,000,000 physical records.

Note: 2,000,000 physical volumes are individually identified in existing automated RM systems; 10,000,000 physical volumes are currently stored in offsite storage facilities.

About 50 metadata elements could potentially be tracked for each physical volume and electronic record (see **Appendix G**)

There are multiple terabytes of GIS and other large scale database information that is regularly used to generate documents and records which must be managed by the EDRMS software. The corporate financial records are in Oracle Financials,

corporate personnel records are in PeopleSoft and there are a few installations of SAP, primarily in Special Operating Agencies such as the Queen's Printer.

Document and Records Management Services

Document and Records Management Services provide a common backbone for addressing the functional requirements identified in this document.

There will be a strong dependence and reliance by the document and record management services on the other application-enabling infrastructure components. For example: messages containing documents as attachments will require:

- An integration of the messaging;
- Record and document management services;
- Access to the document library/repository through a common authentication service;
- Workflow engines handling the flow of approval will need to be coupled with the document and record management services.

There is a requirement for long-term integration with an application for managing physical records in their semi-active state such as ARIS (Archives and Records Information System). The EDRMS will need to incorporate ARIS linking data (accession/application numbers) with potential for future integration.

Workflow Management Services

There will be a requirement for the document and record management services to provide or interface with workflow management systems. More information on the emerging interface standards for workflow management can be found at the Workflow Management Coalition Web site: <http://www.wfmc.org/>.

Database Environment

The BC government database standard is Oracle, although there are installations of Microsoft SQL Server and IBM's DB2. Solutions that meet the database standard will be ranked higher than those that do not.

7.1.3 Key Deliverables

The following are the key deliverables for this project:

- Licenses and all related materials to enable an initial pilot installation in up to four (4) organizations, at four different locations one of which must serve up to 500 users for up to four months. One pilot will be at the BC Assessment Authority. The location of others will be determined after the product selection is complete;
- Appropriate licenses for up to 30,000 users, which will likely be deployed over the next two years. This number is for planning purposes only; the actual number of licenses may be less, and/or the time frame for installation may be longer than currently anticipated;
- Licenses that will allow for multiple server installation where necessary;

- Detailed work plans and estimated timeframes and costs for installation and configuration, including estimated effort required from BC government personnel;
- Suggestions regarding need for a custom *ARCS/ORCS* database;
- Appropriate and sufficient user and technical manuals and other necessary documentation;
- A user training strategy and training materials;
- Necessary customization or integration work to enable the products selected to work together and with existing applications seamlessly together from a user perspective;
- Systems staff training and onsite support provided on an as-and-when-requested basis to guide and support the initial implementation of the software.

7.1.4 Budget

A final budget has not yet been approved for this project because of the difficulty in estimating the cost of licensing the software that is selected and the cost of any custom integration that may be required in order for the solution proposed to work as expected.

The BC government is committed to finalising the budget for this project as soon as possible after the selection of the software. Funds have been identified for pilot project(s) to ensure that there is no undue delay due to the administrative requirements associated with final budget approval.

All funds required after March 2002 are subject to the normal budget reviews and to the voting of the necessary appropriations each fiscal year.

7.1.5 Timing

The government of British Columbia wishes to undertake the pilot implementations early in the 2002 calendar year with the installation of software across government in the fall of 2002 and spring of 2003. Target completion is March 31, 2003, but this may be delayed if there is significant up-front integration needed, if the pilot projects identify issues that need to be resolved before full installation, or if there are unanticipated financial constraints.

Government reserves the right to cancel this RFP and any subsequent Contract at any point up until after the end of the pilot implementation phase if, in its sole judgement, the software does not meet government's performance expectations.

7.1.6 Out of Scope

The following activities are out of scope:

- Services required to convert documents to electronic images and replacement of existing legacy document imaging systems already

installed and operational within the province, but the system selected should be able to manage scanned images and related documents;

- Business process redesign or line of business application development using the selected software;
- Off-site storage, backup and retrieval of electronic records either individually or for repositories containing multiple records;
- Provision, installation and operation of the common infrastructure needed for the EDRMS software – that is servers, network connections, etc. Proponents will be expected to identify what common infrastructure is necessary to run the software being proposed.

7.2 Government Standard

The Chief Information Office and other government organisations regularly conduct reviews of government’s information technology needs and of opportunities to realise benefits through corporate policies and standards. The Province intends that the Enterprise Document and Records Management System selected through this RFP will become the Province’s standard EDRMS software.

8 Evaluation Criteria

8.1 Mandatory

The following are mandatory requirements. Proposals not clearly demonstrating that they meet them will receive no further consideration during the evaluation process.

The proposal must be received at the closing location by the specified closing date and time.
The proposal must be in English and must not be sent by facsimile.
Ten (10) bound copies and one (1) electronic copy of the proposal must be submitted.
Two references must be included for enterprise wide document management and/or records management installations made on behalf of clients using the software proposed for the BC government.
The proposal must be signed by a person authorised to sign on behalf of the Proponent.
The software proposed must be scalable to 30,000+ users.
The software proposed must be able to manage across multiple repositories.
The software proposed must be able to operate across all geographic locations in the province.
The software proposed must support and be compatible with the BC government records classification and scheduling systems (<i>ARCS/ORCS</i>).
The software component of the proposed solution, which will manage electronic records, must be certified against DoD 5015.2. Proponents may recommend combinations of Records Management software and enterprise document management software that are not certified, provided the electronic records management component is certified.

8.2 Desirable

Proposals meeting the mandatory requirements will be further assessed against the following desirable criteria.

Criteria	Maximum Score	Upset Score
<p>1. Company Profile and Experience The project is seeking software tools from a firm that is both innovative and likely to be around in the longer term.</p> <p>A. Proposals should include an overview of the company and provide an annual report or other document that demonstrates the financial viability of the company. The overview should also include a description of the company’s presence on Vancouver Island and Lower Mainland. (5)</p> <p>B. The client references will be asked about the ability of the firm to implement EDMS and RMS applications and the capability of the software to meet our needs. (10)</p>	15	10
<p>2. Price Proponents should supply prices for four things:</p> <p>A. The estimated cost of any custom integration or functionality that is needed to make the software work as expected;</p> <p>B. The estimated cost of any additional components and/or associated deliverables required by the BC government (excluding desktop hardware, servers and network components);</p> <p>C. The estimated per person training costs that will be required to enable full use of the software;</p> <p>D. Licensing costs. These may be a per seat basis, a per server, a per use basis or any other basis the Proponent may wish to offer.</p>	15	11
<p>3. Written Response</p> <p>A. Description (10 page maximum) of the solution proposed (10)</p> <p>B. Appendix F score (35)</p>	45	32
<p>4. Presentation/Demo Only those Proponents who are short-listed will be required to do a presentation/demo.</p>	25	

The point allocation will be according to the standard Purchasing Commission procedure: lowest bid divided by the company bid times the number of points.

*Example: if there are 40 points available and three bids of \$40,000, \$45,000 and \$50,000, points would be allocated as follows – company A $(\$40,000/\$40,000)*40$ or 40 points; company B $(\$40,000/\$45,000)*40$ or 35.6 points; company C $(\$40,000/\$50,000)*40$ or 32 points.*

Following the evaluation of the price and written proposals, up to three of the highest-scoring proponents may be asked to give a presentation/demo of their proposed solution. If there are more than three Proponents that exceed the upset scores, only the highest scoring three will be short-listed.

The presentation will consist of one half hour to describe the product features and up to two and one half hours to demonstrate key features, some of which can be selected by the Proponent, some of which will be provided in advance and some of which will be ad hoc requests during the presentation.

9 Proponent Response

In responding to this RFP, Proponents:

- Should identify any limitations of the proposed software, particularly limitations related to repository management and/or number of documents that can be accommodated;
- Should clearly identify any additional deliverables not included in description of deliverables that the Proponent considers necessary to achieve the scope and objectives of the BC government;
- May wish to indicate how they would expect their products to interact or link to Enterprise-Wide Portal Software.

In order to receive full consideration during evaluation, proposals should include the following:

9.1 To Meet Mandatory Criteria

Enclose a table with each item in Section 8.1 listed with a confirmation that the proposed solution meets the requirement.

9.2 To Meet Desirable Criteria

Proponents should remove the list of Desirable System Requirements presented in **Appendix F**, and indicate by marking the checkbox beside each feature with an “x” or a check mark, each feature supported by their proposed solution. The filled-in **Appendix F** must be submitted with the Proponent’s response. Where explanations are requested, additional sheets may be appended. Each response with additional information should clearly state which question/item the additional information supports.

The description of the proposed solution should not exceed ten pages and should include at least the following: evidence that the Proponent understands the goal/vision that is to be achieved; products being proposed; integration issues; any weakness or shortcoming of the solution and suggestions on how this will be overcome.

10 Proposal Format

The following format and sequence should be followed in order to provide consistency in Proponent response and ensure each proposal receives full consideration. All pages should be consecutively numbered.

Proposal covering letter. Please use sample provided in **Appendix A**.

Table of contents including page numbers including:

Introduction

Company Profile, Experience and References

Description of Proposed Solution

Evaluation Criteria Response (including **Appendix F**)

Pricing

Description of Sub-contracted Work and Sub-contractors (if applicable)

Other

Appendices

Appendix A Proposal Covering Letter

Letterhead or Proponent's name and address

Date

Purchasing Commission
P.O. Box 9476, Stn. Prov. Gov't.
3350 Douglas Street, Suite 102
Victoria, B.C. V8W 9W6

Attention: David Simon

Dear Sir

Subject: **Enterprise Document and Records Management System
Request for Proposal number**

The enclosed proposal is submitted in response to the above-referenced Request for Proposal. Through submission of this proposal we agree to all of the terms and conditions of the Request for Proposal.

We have carefully read and examined the Request for Proposal and have conducted such other investigations as were prudent and reasonable in preparing the proposal. We agree to be bound by statements and representations made in this proposal and to any agreement resulting from the proposal.

Yours truly

Signature

Name: _____

Title: _____

Legal name of Proponent: _____

Date: _____

Appendix B Form of Contract

Selected Contract Clauses

By submission of a proposal, the Proponent agrees that, should it be identified as the successful Proponent, it is willing to enter into a Contract with the Province that may include, at the Province's discretion, the following clauses:

Registration with Workers' Compensation Board

The Contract may contain a provision that the Contractor and any approved sub-Contractors should be registered with the Workers' Compensation Board (WCB), in which case WCB coverage should be maintained for the duration of the Contract. Prior to receiving any payment, the Contractor may be required to submit a WCB Clearance Letter indicating that all WCB assessments have been paid.

Compliance With Laws

The Contractor will give all the notices and obtain all the licenses and permits required to perform the work. The Contractor will comply with all laws applicable to the work or performance of the Contract.

Laws of British Columbia

Any Contract resulting from this Request for Proposal will be governed by and will be construed and interpreted in accordance with the laws of the Province of British Columbia.

Arbitration

All disputes arising out of or in connection with the Contract will, unless the parties otherwise agree, be referred to and finally resolved by arbitration pursuant to the Commercial Arbitration Act.

Indemnity

Any Contract resulting from this Request for Proposal will require that the Contractor indemnify and save harmless the Province, its employees and agents from and against all claims, demands, losses, damages, costs and expenses made against or incurred, suffered or sustained by the Province at any time or times (either before or after the expiration or sooner termination of this Contract) where the same or any of them are based upon or arise out of or from anything done or omitted to be done by the Contractor or by any servant, employee, officer, director or sub-Contractor of the Contractor pursuant to the Contract excepting always liability arising out of the independent acts of the Province.

Insurance

Any Contract resulting from this Request for Proposal may require that the Contractor, without limiting its obligations or liabilities and at its own expense, provide and maintain throughout the Contract term, the following insurances with insurers licensed in British

Columbia in forms acceptable to the Province. All required insurance will be endorsed to provide the Province with 30 days' advance written notice of cancellation or material change. The Contractor will provide the Province with evidence of the required insurance, in the form of a completed Province of British Columbia Certificate of Insurance, immediately following execution and delivery of the Contract.

Comprehensive General Liability in an amount not less than \$1,000,000 inclusive per occurrence insuring against bodily injury and property damage and including liability assumed under the Contract. The Province is to be added as an additional insured and the policy shall contain a cross liability clause.

Professional Liability in an amount not less than \$1,000,000 insuring the Contractor's liability resulting from errors and omissions in the performance of professional services under the Contract.

Automobile Liability on all vehicles owned, operated or licensed in the name of the Contractor in an amount not less than \$1,000,000.

Funding

The Contract and the financial obligations of the Province pursuant to that Contract are subject to:

there being sufficient moneys available in an appropriation, as defined in the Financial Administration Act, to enable the Province in any fiscal year or part thereof when the payment of money by the Province to the Contractor falls due under the Contract entered into pursuant to this Request for Proposal to make that payment; and

Treasury Board as defined in the Financial Administration Act, not having controlled or limited expenditure under any appropriation referred to in subsection a) of this section.

Payment Holdback

The Contract may contain a provision whereby the Province will hold back a portion of the total Contract price until the requirements of the Contract have been met.

Software

It is the Contractor's responsibility to ensure that the Province has all licenses required to use any software that may be supplied by the Contractor pursuant to the Contract.

Intellectual Property Rights

The Province will be the owner of the intellectual property rights, including patent, copyright, trademark, industrial design and trade secrets in any product developed through a Contract. Licensing and marketing rights to the developed product will not be granted in the Contract. Proposals regarding these rights should not be submitted in response to this Request for Proposal and will not be considered in evaluating responses. If, in the future, the Province elects to commercialise the developed product, the licensing and marketing rights will be negotiated separately.

Appendix C Proponent Checklist

This checklist has been provided solely for the convenience of the Proponent. Its use is not mandatory and it does not have to be returned with the proposal. However, the Receipt Confirmation form should be returned upon receipt of the Request for Proposal.

- The requirements of the Request for Proposal have been read and understood by everyone involved in putting together the proposal.
- The Receipt Confirmation Form has been completed and sent in.
- The proposal addresses everything asked for in the Request for Proposal.
- The proposal meets all the mandatory requirements of the Request for Proposal.
- The proposal clearly identifies the Proponent, the project, and the Request for Proposal number.
- The Proponent's name and the Request for Proposal number appear on the proposal envelope.
- The appropriate number of copies of the proposal has been made. (Proposals without the correct number of copies may be rejected.)
- Every care has been taken to make sure the proposals are at the closing location in plenty of time, as late proposals will be rejected.
- The proposal is being delivered by hand, courier, or mail, as faxed proposals are not accepted.

Appendix D Receipt Confirmation Form

Project Title: Enterprise Document and Records
Management System

Closing Date: November 26, 2001

Request for Proposal No. _____

Ministry of Management Services

To receive any further information about this Request for Proposal please return this form to:

Attention: **David Simon**
Purchasing Commission
P.O. Box 9476, Stn Prov Gov't
3350 Douglas Street, Suite 102
Victoria, B.C. V8W 9W6
Fax: **(250) 387-7310**

COMPANY: _____

STREET ADDRESS: _____

CITY/PROVINCE: _____ **POSTAL CODE:** _____

MAILING ADDRESS IF DIFFERENT: _____

PHONE NUMBER: _____ **FAX NUMBER:** _____

CONTACT PERSON: _____

E-MAIL: _____

WE WILL BE SENDING _____ REPRESENTATIVES TO THE PROPONENTS' MEETING.
(NUMBER)

WE WILL NOT BE ATTENDING BUT WILL PROBABLY BE SUBMITTING A PROPOSAL.

UNLESS IT CAN BE SENT BY FAX, FURTHER CORRESPONDENCE ABOUT THIS REQUEST FOR PROPOSAL SHOULD BE SENT BY:

COURIER COLLECT.
PROVIDE COURIER NAME AND ACCOUNT NO: _____

MAIL

SIGNATURE: _____

TITLE: _____

Appendix E High Level Requirements (Records Management)

File: ARCS 420-25/RMBR

Date: June 20, 2001

BC GOVERNMENT RECORDS MANAGEMENT BUSINESS REQUIREMENTS

Prepared by the Records Management Business Requirements Working Group:
(ministry names reflect pre-reorganisation structure)

Drew Smyth (Chair), Ministry Records Officer, Ministry of Environment,
Lands and Parks

Ellinore Barker, Corporate Records Officer, Information, Science and
Technology Agency (ISTA)

Peter Freeman, Manager, Corporate Information Services Branch, Information
Technology Services Division, ISTA

Heather Mackay, Electronic Records Analyst, BC Archives, ISTA

Mary McIntosh, Ministry Records Officer, Ministry of Health

Jaye Pelton, Business Analyst, BC Archives, ISTA

Beth Pitblado, Ministry Records Officer, Ministry of Transportation
and Highways and Records Officer responsible for BC Fisheries

BC Government Records Management Business Requirements

Table of Contents

E1	INTRODUCTION	39
E1.1	WHAT IS A RECORD?	39
E1.2	DOCUMENT VS. RECORD	39
E1.3	WHAT IS RECORDS MANAGEMENT?	40
E1.5	STRUCTURE OF THIS DOCUMENT.....	40
E2	BUSINESS REQUIREMENTS – LOCATION MANAGEMENT	42
E2.1	RECORD CREATION OR RECEIPT	43
E2.2	IDENTIFYING AND DOCUMENTING RECORDS	43
E2.3	PROFILE INFORMATION (METADATA).....	43
E2.4	RECORD MAINTENANCE	44
E2.5	SEARCHING FOR AND RETRIEVING RECORDS	44
E2.6	ACCESS SECURITY	44
E2.7	TRANSFERRING RECORDS TO ANOTHER LOCATION.....	45
E3	BUSINESS REQUIREMENTS – PRESERVATION MANAGEMENT	45
E3.1	PHYSICAL PRESERVATION OF RECORDS	45
E3.2	INTELLECTUAL PRESERVATION OF RECORDS	45
E4	BUSINESS REQUIREMENTS – SCHEDULING MANAGEMENT	46
E4.1	SCHEDULING MANAGEMENT – ACTIVE RECORDS	46
E4.1.1	<i>Records Classification</i>	46
E4.1.2	<i>Active Status</i>	46
E4.1.3	<i>End of Active Status</i>	47
E4.2	SCHEDULING MANAGEMENT – SEMI-ACTIVE RECORDS	47
E4.2.1	<i>Applying Semi-active Retention Schedules</i>	47
E4.2.2	<i>End of Semi-active Status</i>	48
E4.3	SCHEDULING MANAGEMENT – INACTIVE RECORDS	48
E4.3.1	<i>Applying Final Disposition to Inactive Records</i>	48

BC GOVERNMENT RECORDS MANAGEMENT BUSINESS REQUIREMENTS

E1 INTRODUCTION

The *BC Government Records Management Business Requirements* were developed by a working group of ministry records officers, information technology experts, and central agency analysts. They document the functions and requirements for managing records in the BC government.

Note on terminology: The term “record” is defined broadly in the *BC Interpretation Act* (RSBC 1996, c.238) to include “books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is recorded or stored by any means whether graphic, electronic, mechanical or otherwise”. This definition is used in key information management statutes such as the *Document Disposal Act* (RSBC 1996, c. 99) and the *Freedom of Information and Protection of Privacy Act* (RSBC 1996, c. 165) to ensure that the provisions of these statutes apply to all forms of recorded information. However, for the purposes of this RFP, the terms document and records are defined more precisely in order to distinguish between the general functions required to create and maintain documents and the more rigorous controls required to capture and manage documents as business records.

E1.1 What is a Record?

A *record* is a document created or received in the course of government business and maintained for action or reference by an agency as evidence of that business.

- Records exist in all media and formats.
- Email messages and attachments are records.
- If a record is copied, the copy is a new and unique record.

E1.2 Document vs. Record

A document is “recorded information which can be treated as a unit” (*ISO s. 3.10*). Any medium that contains information is a document. A document has the status of a record *only* if it is created or received in the course of government business and if it is maintained as evidence of that business. Most documents created or received by government offices are records.

The BC government must manage all documents in compliance with legal and policy requirements. The *Freedom of Information and Protection of Privacy Act* (RSBC 1996, c. 165) applies to all documents held by government ministries and agencies, whether they are records or not. In addition, all documents are subject to discovery during litigation, regardless of their record or non-record status.

The *Records Management Business Requirements* focus on records and the processes involved in their management. They do not discuss the requirements relating specifically to document management functions. However, records management and

document management are related and important components of an effective information management infrastructure.

E1.3 What is Records Management?

Records management is the exercise of physical and intellectual control over records to ensure their integrity in support of government accountabilities and actions. Ministries establish physical control by ensuring records are identified, documented, located, retrieved, and protected from loss, physical damage or inappropriate access. Ministries establish intellectual control over their records by ensuring they are classified, retained and disposed of (destroyed or transferred to the legal custody of the BC Archives) in accordance with their values (that is, in accordance with retention and disposition schedules). Retaining records required for operational, administrative, fiscal, audit and legal purposes (while applying the final disposition to the records whose primary values have ceased) reduces on-site and off-site storage expenditures.

E1.4 Records Management Legislative and Policy Structure

Records management in the BC government is governed by legislation and policy and supported by established processes and standards.

- The *Document Disposal Act* (RSBC 1996, c. 99) governs the final disposition of government documents (records and non-records) by specifying the approvals required before they may be destroyed, transferred to the custody of the government archives or alienated from the Crown provincial.
- Responsibilities and accountabilities for managing government records are established by Treasury Board policy through the *General Management Operating Policy (GMOP)* and the *Financial Administration Operating Policy (FAOP)* manuals.
- Classification and scheduling systems, such as the government-wide *Administrative Records Classification System (ARCS)* and program-specific *Operational Records Classification Systems (ORCS)*. These systems establish classes of records and determine retention periods and final dispositions that reflect their values.
- The British Columbia Archives (BC Archives) establishes government-wide records management policy through specific guidelines, policies and standards.
- Ministry Records Officers establish ministry policies and procedures in compliance with government-wide policies.

E1.5 Structure of This Document

The *Records Management Business Requirements* cover the physical management of records and the intellectual management of the information contained in records.

Records are subject to actions and processes. They are created, identified, documented, stored, physically transferred, preserved, protected, retained and disposed of. In this document, these actions and processes are addressed in the following three sections: Section 1, “Location Management” relates to the physical management of records in order to access and use them.

Section 2, “Preservation Management” relates to the physical and intellectual maintenance of records in order to preserve the information they contain.

Section 3, “Scheduling Management” addresses how the information contained in records must be managed. Records move through a lifecycle during which they are assigned a status of active, semi-active, or inactive based on a records retention and disposition schedule. This schedule assigns a value to a record that is reflected in its retention period and final disposition. Scheduling management relates to the intellectual management of records in accordance with their values.

In addition, this document contains a glossary of terms (see Definitions, below) that serve to clarify the specific meaning of the terminology used to describe records management business requirements.

Definitions

Terms with specific meaning within the *Business Requirements* document are defined below.

- **Document** is defined as information consigned to a medium. This includes “anything on which there is writing...marks, figures [or] symbols.” (*New South Wales, Australia – Evidence Act 1995*). Documents fall into one of two sub-sets:
 - 1) documents that are also records, or
 - 2) documents that are not records.
- **File** is defined as the logical entity used to organise and manage records. A file manages a group of records that together provide evidence of a complete transaction or a collection of reference material. A file is not a physical entity. Retention and disposition schedules are applied to records at the file level.
- **File Series** is defined as a collection of files that are managed under one primary-secondary classification and have the same scheduling requirements.
- **Final Disposition** is defined as an action applied to eligible files by destroying them, transferring them to the permanent custody of the government archives, or alienating them from the Crown provincial. Files are eligible for final disposition when their active and semi-active retention periods have elapsed. The records schedule designates the appropriate type of final disposition for a file.
- **Life cycle** is defined as the changes of a file’s scheduling status, which moves from active to semi-active to inactive.
- **Location** is defined as the physical location of a file’s volume or volumes. The location of a file’s volumes does not affect the file’s scheduling status.
- **Location management** is defined as managing records so they can be identified, documented, located, viewed, retrieved, copied, and secured from unauthorised access.
- **Preservation management** is defined as managing record media (paper, electronic, micrographic, photographic, cartographic, or any other media) in

order to protect records from loss, damage or degradation. It is also defined as managing recorded information to ensure its authenticity and context as it moves from one media or carrier to another.

- **Record** is defined as “recorded information, in any form...created or received and maintained by an organisation in the transaction of business ...and kept as evidence of such activity.” (*Australian Standard AS 4390-1996, part 1, clause 4.21*) In the BC government, the record is the indivisible unit for records management processes.
- **Records Classification and Scheduling System** organises files into functional groupings for filing and retrieval (classification) and assigns retention periods and final dispositions to classified records (scheduling). These systems are referred to as integrated classification and scheduling systems, as opposed to systems that provide either classification or scheduling but not both. *ARCS* and *ORCS* are examples of integrated systems.
- **Retention and Disposition Schedule** is the length of time a file is to be retained and the type of final disposition that is applied to it. In an integrated classification and scheduling system (*ARCS/ORCS*), retention and disposition schedules are linked to secondary classification numbers.
- **Retention Period** is the length of time a file is retained, and is determined by the retention and disposition schedule. The file may be disposed only after the active and semi-active retention periods that apply to it have elapsed.
- **Scheduling Management** is defined as managing the retention and disposition of files in accordance with their scheduling requirements.
- **Scheduling Status** is defined as the status of a file in accordance with the retention and disposition schedule that applies to it. A file may have a scheduling status of active, semi-active, or inactive. A file is eligible for final disposition when it is inactive.
- **Volume** is defined as a component of a file. A volume contains records, and may exist in any media or format (e.g. file folder, electronic folder, microfilm roll, map drawer, and so on). Volumes are often referred to as folders, enclosures, directories, supplements, or sub-files. All these terms refer to the components of a file, and are covered by “volume” in these *Requirements*.

E2 BUSINESS REQUIREMENTS – LOCATION MANAGEMENT

Ministries must manage their records regardless of media or format or on-site or off-site storage location. Essential to the management of records is the ability to locate, view, retrieve, copy and control access to records, regardless of their scheduling status.

E2.1 Record Creation or Receipt

Upon receipt or creation, records enter the records management system. Records provide documentary evidence of the ministry's activities in performing the functions for which it is responsible.

- A record may be copied, but the act of copying creates a new and unique record.
- Records should be created or received in media or format appropriate to the way they are used and which meets the requirements of their scheduled retention and disposition. If they are not created or received in appropriate media, they must be converted or migrated to appropriate media or format.

E2.2 Identifying and Documenting Records

Records are documented so they can be identified, retrieved and managed. Records in all media and formats must be documented.

- Records must be classified in accordance with an established classification system.
- Ministries must create indexes, file lists, or other finding aids documenting the attributes of all files and their physical components (volumes) to ensure they can be retrieved and the ministry's record holdings are documented.
- Classification and indexing systems must establish and use controlled language.
- All the volumes relating to a file must be documented.
- Documentation may be amended or corrected.
- Documentation must be updated when one or more of a file's volumes are moved.

E2.3 Profile Information (Metadata)

Ministries must maintain profile information for records, volumes and files in order to ensure they can be located. Profile information identifies the unique attributes of records, volumes and files. Attributes include:

- Classification number (the primary-secondary classification)
- Classification title (the primary-secondary title)
- Code and code title, including sub-codes if applicable. Codes differentiate between files with the same classification number in the same office, or are added to a classification number to facilitate retrieval.
- Record date range (the date of the first and last record in each volume of a file, and the first record and last record dates for the entire file)
- Media and/or format (what physical format or formats are the records in?)
- Physical location (where are the records/volumes located? This will include some or all of the following: building, floor, room, shelf or other housing unit, drive, directory, storage media [CD, tape, etc.], container, accession number,

commercial storage facility, or other information relating to the physical location of records and volumes)

- Keywords (words or phrases that allow a user to search for specific files. Depending on technology, keyword searches can be performed by automated records management systems, automated document management systems, automated or manual indexing systems or other methods and tools). Effective keyword searching relies on a controlled vocabulary.

E2.4 Record Maintenance

Files, volumes and records are the components maintained through records management in the BC government.

- A file is not a physical entity. It is the classification and scheduling unit for the records linked to it.
- A volume is a physical entity. It is the physical component of a file.
- A file consists of one or more volumes.
- A volume is maintained in one location.
- Different volumes of one file may be maintained in different locations.
- A volume contains one or more records.
- A record is the indivisible unit for managing recorded information. Records management business requirements do not cover unstructured data or information.

E2.5 Searching For and Retrieving Records

Ministries search for records in order to retrieve and use them. Finding aids must be created and maintained in order to ensure records can be located and retrieved. Finding aids include file lists, box lists, keyword indexes, registers, *ARCS/ORCS* or other attribute information that leads users to the files and records they require. Finding aids may be searched manually or through the use of automated search tools.

E2.6 Access Security

Records in all media or formats must be protected from unauthorized access. This includes records maintained in government offices or on government networks and drives, records maintained in contracted records storage facilities, records maintained on internet or intranet websites, records created by members of the public accessing government services through electronic means, records created by contractors working for government, or other government records maintained in any media or location.

- Access categories must be determined and assigned to record types.
- Access must be restricted in accordance with assigned access categories.
- Designated record documentation (e.g., file lists containing identifying information) must be protected from unauthorised access.
- Records must be protected from unauthorised physical access and unauthorised access through electronic systems.
- Records are located and retrieved by authorised individuals.

E2.7 Transferring Records to Another Location

Records may be transferred from one location to another. A file's volume is the physical entity that is transferred. Hardcopy volumes are physically moved to other locations, and electronic volumes are migrated or transferred. Volumes may be moved within an office, between offices, to and from off-site storage facilities, to and from electronic drives, directories or networks, or temporarily charged out by individuals.

- The new location of a volume must be documented.
- Volumes of one file may be transferred together or individually.
- Accession information must be created and maintained so ministries can locate and access records transferred to off-site storage facilities.

E3 BUSINESS REQUIREMENTS – PRESERVATION MANAGEMENT

Records must be preserved for as long as the provincial government requires them to meet its operational, legal, audit, financial, historical, or other responsibilities. The information maintained on records must also be preserved to ensure it retains its context and authenticity for as long as the government requires the records. Preservation management relates to the physical preservation of record media and the intellectual preservation of recorded information.

E3.1 Physical Preservation of Records

Records must be maintained in a way that protects them from loss, damage, degradation, loss of information, and other threats to their physical integrity and the integrity of the information they contain.

- Records must be maintained on media and in formats that ensure they are readable and accessible for the duration of their active and semi-active retention periods.
- Records scheduled for full or selective retention by the government archives must be maintained on stable media appropriate for permanent retention.
- Records must be housed in environmental conditions that meet their preservation, retrieval and security requirements.
- The record format or media must not compromise the ministry's responsibilities or ability to use the information it contains (e.g., the use of any kind of "lossy" or destructive compression technology that permanently alters the data within the record or datafile, or utilize or introduce additional compression/decompression cycles with data formats that utilise lossy compression techniques).
- Records must be maintained in physical containers appropriate to their media or format.

E3.2 Intellectual Preservation of Records

The context and authenticity of records must be preserved for as long as the government has responsibilities for the information they carry.

- Profile information must be linked to records in a way that ensures they are identifiable and authentic, and the context of their creation and use is maintained.

- Records moved to different media or electronic records moved across carriers must maintain their context and authenticity.

E4 BUSINESS REQUIREMENTS – SCHEDULING MANAGEMENT

Ministries must manage records in accordance with their values. These values are reflected in the retention periods and final dispositions established by *ARCS*, *ORCS*, and other records retention and disposition schedules. Specific individuals are delegated the authority to apply scheduled retention periods and final disposition to records.

A file is linked to a scheduled retention and disposition schedule through a classification number. A file moves through its life cycle over time, its status changing from active, to semi-active to inactive. The scheduling status of a file is determined by its retention and disposition schedule.

The location of the file's volumes does not affect the file's scheduling status.

All records and volumes of a file follow the same retention period and final disposition.

E4.1 Scheduling Management – Active Records

Active status is the first phase of the file's lifecycle. The retention and disposition schedule that applies to the file determines the length of the active phase.

E4.1.1 Records Classification

A record that has been created or received is classified to a file. The file is linked to the retention and disposition schedule through its classification.

- A record is classified and added to a volume. The volume is linked to the file.
- When a file is classified, the appropriate retention and disposition schedule must be applied to it.
- A file is linked to one retention and disposition schedule.
- A classification is linked to one or more retention and disposition schedules.
- The classification function includes determining the office of primary responsibility (OPR) status of the file.
- Different retention and final disposition schedules may be applied to OPR/non-OPR files.

E4.1.2 Active Status

Active status is the first phase of a file's scheduled life cycle.

- A file is opened when the first record is created and filed.
- A file is active until the end of its scheduled active retention period.

- Active status is designated at the file level and applies to all volumes and records within the file.
- The retention and disposition schedule determines the active retention period.
- The scheduled retention and disposition assigned to a file may be changed during its active phase.

E4.1.3 End of Active Status

Files cease to be active when the scheduled active retention period elapses.

- The active retention period may end after a predetermined period of time, or upon the occurrence of a defined trigger event, or when the ministry makes a decision that the file is no longer required for current usage.
- The end of the scheduled active retention period is the “scheduling date” used to calculate when the file is eligible for final disposition.
- The date of the last record of a file may or may not be the same as the date on which the file’s active retention period elapses.
- A file with a semi-active retention period of “nil” (i.e., there is no semi-active retention period) moves to the end of its active and semi-active status at the same time.

E4.2 Scheduling Management – Semi-active Records

When the active retention period elapses, a file’s scheduling status changes to semi-active. Semi-active status is designated by the records retention and disposition schedule. Ministries retain their responsibilities for and legal custody of semi-active records.

E4.2.1 Applying Semi-active Retention Schedules

The date the active retention elapses and the file becomes semi-active is called the “scheduling date”. This date is used to calculate how long the file is retained and when it is eligible for final disposition.

- The semi-active retention period is determined by the schedule.
- A file must be retained for the entirety of its semi-active retention period.
- A file should not be retained past the end of its semi-active retention period.
- Semi-active retention periods are applied at file level. All volumes within a file will have the same scheduling status and be retained for the same period of time.
- When files are stored in fixed containers, the semi-active retention period is the same for the entire container.
- A semi-active file may be reactivated back to active status.

- The scheduled retention and final disposition of a file can be changed while it is semi-active.

E4.2.2 End of Semi-active Status

Files and file volumes reach the end of their semi-active retention period.

- A file changes status from semi-active to inactive when its semi-active retention period elapses.
- All volumes within a file change status at the same time.

E4.3 Scheduling Management – Inactive Records

When the scheduled semi-active retention period has elapsed, a file reaches inactive status. An inactive file is eligible for scheduled final disposition. The type of final disposition is determined by the records retention and disposition schedule. Final disposition types are:

- destruction,
- transfer to the legal custody of the government archives, or
- alienation of the records from the Crown provincial.

E4.3.1 Applying Final Disposition to Inactive Records

Scheduled final disposition is applied to all volumes of a file. Final disposition should be applied to a file when it is eligible (once it has reached inactive status), unless a halt or hold to final disposition action is required.

- Final disposition actions applied to files must be documented.
- Final disposition action can be halted or deferred if the inactive file is required past its eligible disposition date for litigation or for freedom of information requests.
- A designated individual must authorise final disposition.
- When files are stored in fixed containers, final disposition is applied to the entire container.

Appendix F Desirable System Requirements

Table of Contents

F1. ASSUMPTIONS AND GENERAL REQUIREMENTS	51
F1.1. COTS SOLUTION.....	51
F1.2. ENTERPRISE-WIDE SCOPE	51
F1.3. INTERFACES WITH OTHER CENTRAL IM APPLICATIONS	52
F1.4. INTEGRATED MANAGEMENT OF ELECTRONIC AND PHYSICAL RECORDS	52
F2. CLASSIFICATION AND SCHEDULING SYSTEM INTERFACE.....	53
F2.1. ARCS/ORCS DATABASE AND LEGACY SYSTEMS	53
F3. RECORD CREATION AND USE.....	54
F3.1. CREATING FILES AND VOLUMES	54
F3.2. RECORD CREATION/RECEIPT AND CAPTURE	54
F3.3. REDACTION (CREATION OF RECORD EXTRACTS).....	58
F3.4. BATCH IMPORTING	59
F3.5. CLASSIFYING RECORDS	59
F3.6. METADATA.....	60
F3.7. ORGANIZATIONAL INFORMATION AND LINKAGES	63
F3.8. SEARCHING AND RETRIEVING RECORDS.....	65
F3.9. TRANSFERRING RECORDS TO ANOTHER LOCATION.....	67
F4. SCHEDULING MANAGEMENT	68
F4.1. MANAGING RECORDS SCHEDULES	68
F4.2. APPLYING RETENTION PERIODS, INCLUDING REVIEW AND APPROVAL	70
F4.3. DISPOSITION AND TRANSFER/EXPORT	72
F5. PRESERVATION AND ONGOING ACCESS	76
F6. SECURITY	77
F6.1. DELETION OF RECORDS	77
F6.2. RECORDS SECURITY CATEGORIES	78
F6.3. USER ACCESS/AUTHENTICATION	78
F6.4. AUDIT.....	80
F6.5. BACKUP AND RECOVERY.....	82
F6.6. VITAL RECORDS	82
F7. PRINTING AND REPORTS.....	82
F7.1. PRINTING.....	82
F7.2. REPORTS.....	83
F7.3. LABELLING.....	84
F8. ADMINISTRATIVE FUNCTIONS.....	84
F8.1. GENERAL SYSTEMS ADMINISTRATION	84
F8.2. ADMINISTRATIVE REPORTS	85
F9. DOCUMENT MANAGEMENT	86
F9.1. GENERAL REQUIREMENTS	86
F9.2. INTERACTION WITH RM FUNCTIONS	87

F10. OTHER FUNCTIONALITY 88

- F10.1. WORKFLOW 88
- F10.2. ELECTRONIC SIGNATURES 90
- F10.3. ENCRYPTION..... 90
- F10.4. ELECTRONIC WATERMARKS..... 91

F11. GENERAL REQUIREMENTS..... 91

- F11.1. EASE OF USE..... 91
- F11.2. PRODUCT MATURITY AND CURRENCY 93
- F11.3. SCALABILITY 94
- F11.4. PERFORMANCE 95
- F11.5. OPENNESS, CONNECTIVITY AND STANDARDS 96

F12. TECHNICAL REQUIREMENTS 98

- F12.1. ABILITY TO OPERATE WITHIN BC GOVERNMENT TECHNOLOGY INFRASTRUCTURE..... 98

F1. Assumptions and General Requirements

The Enterprise Document and Records Management System (EDRMS) will be expected to have the basic characteristics and capabilities outlined below.

The ability of the proposed EDRMS solution to meet these general requirements and other specific requirements will be evaluated on the basis of the responses given in sections F.2 - F.12.

Proponents are asked to check each requirement that the proposed solution can meet. Where narrative responses are requested, Proponents are asked to attach explanatory information.

Note: sources used in compiling these requirements include the:

- *European Commission's Model Requirements for the Management of Electronic Records* <http://www.cornwell.co.uk/moreq> (cited as **MoReq**);
- *Public Record Office's Functional Requirements for Electronic Records Management Systems* <http://www.pro.gov.uk/recordsmanagement/eros/invest/default.htm> (cited as **PRO**); and
- *Association for Information and Image Management's Implementation Guidelines and Standards Associated with Web-Based Document Management Technologies* http://stnds.aiim.wegov2.com/file_depot/0-10000000/0-10000/1462/folder/10666/AIIM+ARP1+2000.pdf (cited as **AIIM**).

F1.1. COTS Solution

The EDRMS will consist of a single suite of commercial, off the shelf applications covering required document and records management functions for both electronic and physical records, with full integration among application components.

Note: Unless otherwise indicated, the requirements specified in this appendix apply to the EDRMS as a whole. The requirements may be met with a single application or a combination of separate applications (e.g., applications for document management, management of electronic records, and management of physical records, etc.) comprising the integrated EDRMS suite.

F1.2. Enterprise-Wide Scope

For each defined BC government organization (e.g., each ministry), the EDRMS will support integrated management of all common forms of electronic office records (e.g., MS Office and Outlook records) and all forms of hardcopy records. The EDRMS will be extensible to cover other electronic record types (images, database reports, voicemail, etc.).

The EDRMS will support easy transfer of records and records information (metadata) among organizations (e.g., from one ministry to another during government re-organizations).

The EDRMS will enable on-line searching of records information across organizations and across records repositories throughout the BC government.

F1.3. Interfaces with Other Central IM Applications

Records scheduling and classification data is expected to be maintained on a central, government-wide *ARCS/ORCS* database, external to the EDRMS. The EDRMS suite will seamlessly interface with or use the data contained in the *ARCS/ORCS* database for its records classification and scheduling functions.

Data and processes for the management of records stored in offsite facilities (BC Archives Records Centre Services) and the management of archival records will continue to be maintained in the BC Archives ARIS (Archives and Records Information System) application. The EDRMS will maintain specified data described in these requirements that will be drawn from or provided to ARIS and will have the potential for additional future integration with ARIS.

The EDRMS will provide the BC government with a common document and records management infrastructure, integrated with the current standard office applications and infrastructure and with current/emerging document-related applications.

F1.4. Integrated Management of Electronic and Physical Records

The EDRMS will support management of both electronic and physical records in accordance with the existing BC government IM governance requirements (see section 6) and the records management business requirements defined in **Appendix E**.

The EDRMS will enable the authenticity, integrity and accessibility of electronic records to be maintained over time (e.g., decades), across systems (e.g., migrations to new versions of the EDRMS software; export to other systems) and across formats (e.g., export to non-proprietary formats for archival preservation).

The EDRMS will support BC government requirements and processes for the management of physical records and the batch transfer of records containers to central offsite storage facilities and/or BC Archives archival custody.

The EDRMS will maintain standard metadata about electronic and physical files and volumes (including hybrid files consisting of both electronic and physical volumes); will maintain standard metadata about records (i.e., as records profiles); will maintain audit trails of actions taken on records; and will ensure security of records.

F2. Classification and Scheduling System Interface

F2.1. ARCS/ORCS Database and Legacy Systems

- F2.1.1. The EDRMS should use an external master *ARCS/ORCS* database for all records classification data (e.g., primary and secondary data elements) and scheduling data (e.g., records retention periods and disposition categories). The EDRMS should do this by:
- F2.1.1.1. interoperating with the *ARCS/ORCS* database (i.e., incorporate direct “live” connections to the *ARCS/ORCS* tables as part of the EDRMS);
- F2.1.1.2. interfacing with the *ARCS/ORCS* database and downloading required data to the EDRMS as a regular (e.g., monthly), automatic operation requiring minimal data revision in the EDRMS;
- F2.1.1.3. batch importing an initial data set, that must be revised and maintained within the EDRMS; or
- F2.1.1.4. using other means for entering and maintaining *ARCS/ORCS* data within the EDRMS (provide explanation below).

Note: Proponents can evaluate the main types of classification and scheduling data used in ARCS by reviewing ARCS Online <http://www.bcarchives.gov.bc.ca/arcs/index.htm>. Similar data are used in ORCS and other BC government records schedules. Appendix H provides a brief description of the envisaged structure of the ARCS/ORCS database, planned as central application for developing, reviewing/approving, and electronically publishing the master copies of all ARCS, ORCS and other BC government continuing records schedules.

F2.1.2. The EDRMS should support use of:

- F2.1.2.1. multiple records classification and scheduling schemes (e.g., multiple *ORCS*) within a single record repository;
- F2.1.2.2. a single records classification and scheduling scheme (e.g., *ARCS* or a single *ORCS*) across a network of electronic record repositories. (Based on MoReq 3.1.9)
- F2.1.3. The EDRMS should support bulk importing of legacy *ARCS/ORCS* scheduling data from existing BC government automated records management systems.

ATTACH AN EXPLANATION OF THE PROPOSED APPROACH FOR MEETING THE ABOVE REQUIREMENTS; E.G.:

- **ABILITY OF THE PROPOSED EDRMS APPLICATION TO MEET THE REQUIREMENT “OUT OF THE BOX”;**
- **REQUIRED APPLICATION CUSTOMIZATION;**
- **NATURE OF REQUIRED REVISIONS/MAINTENANCE OF ARCS/ORCS DATA WITHIN THE EDRMS;**

- **ANY DATA OR FUNCTIONAL CHARACTERISTICS OF ARCS/ORCS WHICH CANNOT BE READILY SUPPORTED BY THE PROPOSED SOLUTION;**
- **ABILITY TO PERFORM REQUIRED ARCS/ORCS DEVELOPMENT, MAINTENANCE AND PUBLICATION FUNCTIONS WITHIN THE EDRMS (I.E., ELIMINATING NEED FOR AN EXTERNAL CENTRAL DATABASE);**
- **OTHER RELEVANT CONSIDERATIONS.**

F3. Record Creation and Use

F3.1. Creating Files and Volumes

- F3.1.1. The EDRMS should support the management of records at the file/volume level (hard copy records organized into files/volumes, but not necessarily registered individually) or at the file/volume and record levels (electronic records and hardcopy records that are registered individually).
- F3.1.2. The EDRMS should restrict the entry of new files in the system to authorized users.
- F3.1.3. The EDRMS should support automatic creation of a volume when a file is created.
- F3.1.4. The EDRMS should permit a file to have multiple subordinate volumes.
- F3.1.5. The EDRMS should permit a file to have multiple subordinate volumes open concurrently (i.e., multiple active volumes).
- F3.1.6. The EDRMS should allow an authorised user to re-open a previously closed volume temporarily for the addition of records, and subsequently to close that volume again. (Based on MoReq 3.3.6)
- F3.1.7. The EDRMS should support automatic “roll over” of cyclical files (e.g., files that are closed at the end of a calendar or fiscal year and need to be replaced with new files for the following year covering the same subject matter).
- F3.1.8. The EDRMS should allow for the automatic creation and maintenance of a list (or “repertory”) of files. (Based on MoReq 3.2.10)
- F3.1.9. The EDRMS should define in the file repertory physical files and volumes, and should allow the presence of physical records in these volumes to be reflected and managed in the same way as electronic records. (Based on MoReq 10.1.1)
- F3.1.10. The EDRMS should support the management of “hybrid” files containing electronic and physical components, and allow the components to be managed in an integrated manner. (Based on MoReq 10.1.2)
- F3.1.11. The EDRMS should allow a different metadata element set to be configured for physical files and electronic files; physical file metadata should include information on the physical location of the physical file. (Based on MoReq 10.1.4)

F3.2. Record Creation/Receipt and Capture

- F3.2.1. The EDRMS should enable documents to be captured as records by assigning records registration numbers and establishing profile metadata for the records.

- F3.2.1.1. The EDRMS should support the registration of electronic records.
- F3.2.1.2. The EDRMS should support the registration of physical records.
- F3.2.1.3. The EDRMS should be capable of creating profiles for electronic records.
- F3.2.1.4. The EDRMS should be capable of creating profiles for physical records.
- F3.2.2. The EDRMS capture process should provide the functionality to:
 - F3.2.2.1. register and manage all electronic records regardless of the method of encoding or other technological characteristics;
 - F3.2.2.2. ensure that the records are associated with a classification scheme and can be associated with one or more files;
 - F3.2.2.3. integrate with the application software that generates the records (where possible);
 - F3.2.2.4. validate and control the entry of metadata into the EDRMS. (Based on MoReq 6.1.1).
- F3.2.3. The EDRMS should capture in the electronic records management environment:
 - F3.2.3.1. the content of the electronic record, including information defining its form and rendition and information defining the structure and behaviour of the electronic record, retaining its structural integrity (for example, all the components of an e-mail message with attachment(s), or of a web page, with their links);
 - F3.2.3.2. information about the electronic document, for example, the file name;
 - F3.2.3.3. the date of creation and other document metadata about the elements of the record;
 - F3.2.3.4. information about the context in which the electronic record was originated, created and registered, for example its business process and, originator(s), author(s);
 - F3.2.3.5. information about the application program, which generated the record, including its version. (Based on MoReq 6.1.2)
- F3.2.4. The EDRMS should allow the capture acquisition of metadata elements specified at systems configuration, and retain them with the electronic record in a tightly-bound relationship at all times. (Based on MoReq 6.1.3)
- F3.2.5. The EDRMS should ensure authorized users and administrators only can change the content of selected elements of the metadata of the electronic record. (Based on MoReq 6.1.4)
- F3.2.6. The EDRMS should support the ability to assign the same electronic records to different electronic files, from one electronic document without physical duplication of the electronic record. (Based on MoReq 6.1.5)

- F3.2.7. The EDRMS should support automated assistance in registration of electronic documents, by automatically extracting metadata for as many types of documents as possible, including at least the following document types:
 - F3.2.7.1. office documents (e.g., word-processed letters in a standard format);
 - F3.2.7.2. e-mail without attachments, both incoming and outgoing;
 - F3.2.7.3. e-mail with attachments, both incoming and outgoing;
 - F3.2.7.4. facsimile messages, both incoming and outgoing. (Based on MoReq 6.1.6; 6.1.14)

- F3.2.8. The EDRMS should record the date and time of registration as metadata. (Based on MoReq 6.1.7)

- F3.2.9. The EDRMS should ensure that every registered record has a viewable registry entry that includes metadata specified at configuration time. (Based on MoReq 6.1.8)

- F3.2.10. The EDRMS should allow entry of further descriptive and other metadata at the time of registration and/or at a later stage of processing. (Based on MoReq 6.1.9)

- F3.2.11. Where a document has more than one version, the EDRMS should allow users to choose at least one of the following:
 - F3.2.11.1. register one version of the document as a record;
 - F3.2.11.2. register each version of the document as a record;
 - F3.2.11.3. register all versions of the document as one record. (Based on MoReq 6.1.10)

- F3.2.12. The EDRMS should allow a user to pass electronic records to another user to complete the process of capture. (Based on MoReq 6.1.12)

- F3.2.13. For electronic records that are constructed of more than one component, the EDRMS should provide the following functions:
 - F3.2.13.1. handle the record as a single indivisible record, retaining the relationship between the components;
 - F3.2.13.2. retain the record's structural integrity;
 - F3.2.13.3. support later integrated retrieval, display, management;
 - F3.2.13.4. manage disposal of all components of the electronic record as a whole unit (i.e., in one operation). (Based on MoReq 6.1.13)
 - F3.2.13.5. The EDRMS should issue a warning if a user attempts to register a document that has already been registered in the same file. (Based on MoReq 6.1.15)

- F3.2.14. The EDRMS should support the capture of common forms of BC government office documents as records. These include both simple and compound document format types; e.g.:
- F3.2.14.1. Simple: wp documents, presentations, spreadsheets (at minimum, all MS Office document types); e-mail messages (at minimum, MS Outlook); text, images, facsimiles ;
 - F3.2.14.2. Compound: electronic mail with attachments, desktop publishing, web pages, graphics, “layered” documents generated from database or GIS applications. (Based on MoReq 6.3.2)
- F3.2.15. The EDRMS should support the ability to capture completed forms, including both the form content and the original structure of the form at the time of data entry.
- F3.2.16. The document formats supported should be extendable as new formats are introduced. (Based on MoReq 6.3.3)
- F3.2.17. The EDRMS should be able to capture the following types of documents:
- F3.2.17.1. electronic calendars;
 - F3.2.17.2. information from other computer applications e.g., Accounting, Payroll, Computer Aided Design, GIS;
 - F3.2.17.3. scanned paper documents;
 - F3.2.17.4. voice files;
 - F3.2.17.5. video clips;
 - F3.2.17.6. digital schematics and maps;
 - F3.2.17.7. structured data (e.g., EDI transactions);
 - F3.2.17.8. databases;
 - F3.2.17.9. multimedia documents. (Based on MoReq 6.3.4)
- F3.2.18. The EDRMS should not impose any practical limit on the number of records, which can be captured in a file, or on the number of records, which can be stored in the EDRMS. (Based on MoReq 6.3.5)
- F3.2.19. The EDRMS should allow a compound document to be captured in either of two ways:
- F3.2.19.1. as a single compound record;
 - F3.2.19.2. as a series of linked simple records, one per component of the compound document. (Based on MoReq 6.3.6)

- F3.2.20. The EDRMS should provide seamless integration with, and continued support for, existing document creation and filing tools, such as MS Word and Windows Explorer, etc.
- F3.2.20.1. For example, when using MS Word/Explorer, etc. with records in the EDRMS repository, the File Open command should result in check-out; the File Save command should result in check in.
- F3.2.20.2. The EDRMS should allow users to process and capture their incoming e-mail messages from within their e-mail system. The user should be able to process each e-mail in the inbox, from within their e-mail system, as follows:
- F3.2.20.3. view each mail message and an indication of its attachments (if any);
- F3.2.20.4. view the contents of the attachments using multi-format document viewer;
- F3.2.20.5. register the mail message and its attachments as a new record in EDRMS;
- F3.2.20.6. link the mail message and its attachments to an existing record in EDRMS. (Based on MoReq 6.4.2).

F3.3. Redaction (Creation of Record Extracts)

It is sometimes necessary to make available records containing sensitive information. In such cases, there may be a need to remove the sensitive information, without affecting the underlying record. The process is referred to here as redaction, and the EDRMS should store both the original record and the redacted copy, which is called an 'extract' of the record.

- F3.3.1. The EDRMS should allow authorized users to take a copy of a record, for the purposes of redaction. (Based on MoReq 9.3.9)
- F3.3.2. The EDRMS should provide functionality for removing or hiding sensitive information from the extract, to include at least:
- F3.3.2.1. removal of individual pages of a multi-page image record;
- F3.3.2.2. addition of opaque rectangles to obscure sensitive names or words
- F3.3.2.3. other means of hiding or extracting sensitive information;
- F3.3.2.4. any other features required for video or audio formats if present. (Based on MoReq 9.3.10)
- F3.3.3. If the proposed EDRMS does not provide the above functionality, it should integrate with other software packages to do so. (Based on MoReq 9.3.10)
- F3.3.4. The EDRMS should ensure that none of the removed or hidden information could ever be seen in the extract. (Based on MoReq 9.3.10)
- F3.3.5. When an extract is created, the EDRMS should record its creation in the record's metadata, including at least date, time, reason for creation and creator. (Based on MoReq 9.3.11)

- F3.3.6. The EDRMS should prompt the creator of an extract to assign it to a file. (Based on MoReq 9.3.12)
- F3.3.7. The EDRMS should store a cross-reference to an extract in the same file and volume as the original record, even if that file volume is closed. (Based on MoReq 9.3.13)

F3.4. Batch Importing

- F3.4.1. The EDRMS should provide the capability for authorized individuals to bulk load, as a minimum, pre-existing:
 - F3.4.1.1. file and volume records;
 - F3.4.1.2. electronic records;
 - F3.4.1.3. records profiles.
- F3.4.2. The EDRMS should provide the ability to capture transactional documents generated by other systems. This should include:
 - F3.4.2.1. supporting predefined batch file transaction imports;
 - F3.4.2.2. providing edit rules to customize the automatic registration of the records;
 - F3.4.2.3. maintaining data integrity validation. (Based on MoReq 6.2.1)
- F3.4.3. The EDRMS system should provide facilities to manage input queues. (Based on MoReq 6.2.2)
- F3.4.4. The EDRMS should be able to set up multiple input queues for different document types. (Based on MoReq 6.2.3)

For example, in different environments, queues might be for e-mails, scanned correspondence, documents from a department, group or individual, transactions from computer applications, or documents from other document/content management systems.

F3.5. Classifying Records

- F3.5.1. The EDRMS should be capable of ensuring that all records are classified and scheduled in accordance with the established *ARCS/ORCS* classification schemes.

- F3.5.2. The EDRMS should allow user determination of classifications applied to records when they are classified and registered into the system. The system should provide classification assists for users including some or all of the following:
- F3.5.2.1. making subsets of classification schemes accessible to users or roles;
 - F3.5.2.2. storing lists of recently used classifications or files for users or roles;
 - F3.5.2.3. suggesting the most recently used classifications or files by users;
 - F3.5.2.4. suggesting classifications or files that contain related electronic records;
 - F3.5.2.5. suggesting classifications or files by inference drawn from record metadata elements; for example, significant words used in the document title;
 - F3.5.2.6. suggesting classifications or files by inference from record contents. (Based on MoReq 6.1.11)
- F3.5.3. The EDRMS should provide an “intelligent” engine for the above classification/filing suggestions that can:
- F3.5.3.1. “learn” from past choices made by the user and improve it’s ability to suggest correct classifications or files
 - F3.5.3.2. be configured to auto-classify/auto-file records when a user-specified accuracy level is achieved (e.g., auto-classify if a specified accuracy level is possible, otherwise flag for manual classification).
- F3.5.4. The EDRMS should permit users to move easily between the classification schemas (e.g., primary and secondary records) and lists of existing files when determining appropriate classifications.
- F3.5.5. The EDRMS should identify any existing files under a chosen classification.
- F3.5.6. The EDRMS should permit the reclassification of records or files. If a file is reclassified, the EDRMS should ensure the revised data cascades to volumes and, if required, records.
- F3.5.7. The EDRMS should support the classification or reclassification of multiple files in one operation.
- F3.5.8. The EDRMS should allow users to create cross-references (e.g., “see also” type links) between related files. (Based on MoReq 3.4.11)

F3.6. Metadata

- F3.6.1. The EDRMS should support the designation of metadata by authorized users/administrators.
- F3.6.2. The EDRMS should allow specific sets of metadata elements to be defined for different kinds of records at configuration time. (Based on MoReq 12.1.3)
- F3.6.3. The EDRMS should restrict the ability to make changes to metadata values to authorized users.

- F3.6.4. The EDRMS should support the recording of file and volume metadata when a file is created.
- F3.6.5. The EDRMS should support the entry of the types of file/volume metadata specified at **Appendix G.3**.
- F3.6.6. In particular, file/volume metadata should include:
 - F3.6.6.1. file first record date and file last record date (the date range of the file contents; ideally, cascaded up from volume date ranges);
 - F3.6.6.2. volume first and last record dates (the date range of the records within the volume);
 - F3.6.6.3. file schedule trigger date; i.e., the date from which the eligible disposition date is calculated. It should be possible for the schedule trigger date to be different than the file last record date or the file closure date.
- F3.6.7. The EDRMS should support bulk updates of profile information based on specified criteria. The EDRMS should support batch input and acquisition of profile information (e.g., to a series of files, or a group of records, or multiple volumes of a file).
- F3.6.8. The EDRMS should not present any practical limitation on the number of metadata elements allowed for each item (e.g., file, volume, record). (Based on MoReq 12.1.1)
- F3.6.9. Where the contents of a metadata element can be related to the functional behavior of the EDRMS, the EDRMS should use the contents of that element to determine the functionality. (Based on MoReq 12.1.2)

For example, if the EDRMS stores security categories of records and also stores the security clearance of users, then it should use the latter to determine whether a user can or cannot access a record. If the EDRMS only stores the clearances and categories as text fields which are not used to control access, this requirement is not met.

- F3.6.10. The EDRMS should support at least the following metadata element formats:
 - F3.6.10.1. alphabetic;
 - F3.6.10.2. alphanumeric;
 - F3.6.10.3. numeric;
 - F3.6.10.4. date;
 - F3.6.10.5. logical (i.e., yes/no, true/false). (Based on MoReq 12.1.5).
- F3.6.11. The EDRMS should support the ability to extract metadata elements automatically from records when they are captured. (Based on MoReq 12.1.9)

Examples are the automatic extraction of dates, titles, recipient names and reference numbers from word processed documents or structured transaction documents such as invoices.

- F3.6.12. The EDRMS should allow the Administrator to define at configuration time whether each metadata element is mandatory or optional and whether it is searchable. (Based on MoReq 12.1.4)

- F3.6.13. Where metadata element values are entered manually, the EDRMS should support persistent default values, which are user-definable. (Based on MoReq 12.1.16)

A persistent default appears as the default in the data entry field for each item in succession until a user changes it. Once changed, the new value remains, i.e., becomes persistent.

- F3.6.14. The EDRMS should allow configuration such that any metadata element can be used as a search field in a non-structured search (e.g., a free text search). (Based on MoReq 12.1.17)

F3.6.15. The EDRMS should be able to acquire metadata from:

- F3.6.15.1. the document-creating application package or operating system or network software;
- F3.6.15.2. the user at the time of capture or registration;
- F3.6.15.3. rules defined at configuration time for generation of metadata by the EDRMS at the time of registration. (Based on MoReq 12.1.22)

- F3.6.16. The EDRMS should allow the values of metadata to be provided automatically from the next higher level in the classification scheme hierarchy. (Based on MoReq 12.1.11)

For example, for a volume, the value of some of the metadata elements should be inherited from its parent file; and for a record, the value of some metadata may be inherited from the volume into which it is stored.

- F3.6.17. When changes are made to the ARCS/ORCS database that affect file-level information, the EDRMS should support a prompt that flags changes, and requires authorized approval to initiate the cascade.

- F3.6.18. The EDRMS should support validation of metadata when users enter the metadata, or when it is imported. Validation should use at least the following mechanisms:

- F3.6.18.1. format of the element contents;
- F3.6.18.2. range of values;
- F3.6.18.3. validation against a list of values maintained by the Administrator;
- F3.6.18.4. a valid classification scheme reference. (Based on MoReq 12.1.13)

An example of format validation is that the contents are all numeric, or are in a date format (Based on MoReq 12.1.5)

An example of range format validation is that the contents fall in the range between 1 January 1999 and 31 December 2001. An example of validation against a list of values is verifying that an export destination is present on a list.

- F3.6.19. The EDRMS should support validation of metadata elements using check digit algorithms. (Based on MoReq 12.1.14)

For example, files may be identified by a sixteen-digit credit card number, of which the last digit is a check digit computed from the other fifteen digits using the mod 10 algorithm. Provision of

an application program interface for this feature, allowing organisations to introduce their chosen algorithm, should normally be considered acceptable.

- F3.6.20. The EDRMS should, where required, support validation of metadata using calls to another application (e.g., to a personnel system to check whether a personnel number has been assigned, or to a postal code database system). (Based on MoReq 12.1.15)
- F3.6.21. The EDRMS should ensure that volumes and records retain their unique identification regardless of location or scheduling status. E.g.:
 - F3.6.21.1. volumes batched within an accession for offsite transfer should retain their individual identity in the batch and it should be possible to remove the volumes from the accession without undue effort.
- F3.6.22. The EDRMS should support BC Archives records centre processes for transferring physical records to off-site storage facilities. For example, it should support the entry of the types of off-site transfer metadata specified at **Appendix G.4**.
- F3.6.23. In particular, offsite transfer metadata should include:
 - F3.6.23.1. accession number (7 digit number assigned that identifies one or more batches of containers/volumes transferred offsite; number is generated by BC Archives ARIS system) ;
 - F3.6.23.2. application number (6 digit service application number identifies a particular batch of containers/files transferred offsite under an accession number; number is issued on BC Archives service application forms);
 - F3.6.23.3. container number (10 digit number; comprised of the 6 digit accession number followed by a 4 digit box number; e.g. 920345-0013).
- F3.6.24. Once physical volumes are boxed, the EDRMS should support a simple method of recording the container number in the metadata for each boxed volume (i.e., ability to select multiple volumes and record the box number in a single operation).

F3.7. Organizational Information and Linkages

- F3.7.1. The EDRMS should be able to use the ARIS name authority tables (see **Appendix H.4**) as a control source for organizational names. The EDRMS should do this by:

- F3.7.1.1. interoperating with the ARIS tables;
- F3.7.1.2. interfacing with the ARIS tables and downloading required data to the EDRMS as a regular (e.g., monthly), automatic operation requiring minimal data revision in the EDRMS;
- F3.7.1.3. batch importing an initial data set, that must be revised and maintained within the EDRMS; or
- F3.7.1.4. using other means for entering and maintaining ARIS name records within the EDRMS.
- F3.7.1.5. At minimum, the EDRMS should be capable of associating ARIS name ID numbers (8 digit numeric field) with name records maintained within the EDRMS.

Note: The following requirements apply whether the EDRMS utilises ARIS name records or uses another method to maintain a controlled source of organisational names.

- F3.7.2. The EDRMS should be able to identify BG government organizational units and the responsibilities/roles they hold/perform for particular records or groups of records (e.g., records legal custodian, records creator, Office of Primary Responsibility (OPR)).
- F3.7.3. The EDRMS should be able to maintain/use multi-level name records for BC government organizations down to at least 8 levels; e.g., a record for each ministry, division, branch, section, unit, office, etc., ideally with each name record:
 - F3.7.3.1. linked to the higher and lower level name in a parent/child relationship;
 - F3.7.3.2. linked to predecessor and successor names to track changing organizational structures over time.
- F3.7.4. The EDRMS should be able to use the organizational name records to provide the types of organizational metadata elements specified in **Appendix G**; e.g.:
 - F3.7.4.1. current legal custodian (owner), creator, and/or OPR names for files/volumes/records
 - F3.7.4.2. transferring agent names for applications/accessions (names of offices transferring batches of records to offsite storage)
- F3.7.5. The EDRMS should support the assignment of files to an organizational unit (e.g., identifying the organization as having legal custody or other specified responsibility for the files).
- F3.7.6. The EDRMS should enable users to specify and use generic terms (e.g., central office, field office) to identify OPRs or other organizational responsibilities, where it is not feasible to use a specific organization name.
- F3.7.7. The EDRMS should support efficient bulk moves of files/volumes/records and their metadata from one organizational unit to an inheriting organizational unit.
- F3.7.8. The EDRMS should support batch changes of organizational metadata (e.g., changes to the name of the current legal custodian for files/records transferred from one organization to another).

- F3.7.9. If there is a change of legal custody, the EDRMS should ensure organizational metadata for files/volumes/records is updated while maintaining a history of past legal custodians.
- F3.7.10. The EDRMS should allow Administrators to make changes to the organizational name records and file repertory, ensuring all metadata and audit trail data are handled correctly and completely at all times, in order to reflect the following kinds of organizational change:
- F3.7.10.1. division of an organizational unit into two or more units;
 - F3.7.10.2. combination of two or more organizational units into one;
 - F3.7.10.3. movement or re-naming of an organizational unit;
 - F3.7.10.4. division of a whole organization into two or more organizations. (Based on MoReq 9.1.6)
 - F3.7.10.5. The EDRMS should support the movement of User IDs between organizational units, and any changes to access authority. (Based on MoReq 9.1.7)

F3.8. Searching and Retrieving Records

This section describes the functionality required to search for records and/or their metadata, and to display the records/metadata.

Searching

- F3.8.1. The EDRMS should support enterprise-wide searching; i.e., a user with the requisite permissions should be able to conduct:
- F3.8.1.1. searches of the records of an entire organizational unit
 - F3.8.1.2. *concurrent* searches of records across multiple organization units and/or records repositories (e.g., users do not need to conduct separate searches for each organization unit or repository but rather can search across an entire ministry or across multiple ministries).
- F3.8.2. The EDRMS search mechanisms should be integrated and should, to users, appear the same for all classification levels. (Based on MoReq 8.1.2)
- In other words, users should see the same interface, features and options whether searching for ARCS/ORCS classifications, files or records.*
- F3.8.3. The EDRMS should support searches of the classification system.
 - F3.8.4. The EDRMS should allow the metadata of any object (such as record, volume, file or primary and secondary) to be searched, using the techniques in this section. (Based on MoReq 8.1.19)
 - F3.8.5. The EDRMS should support searches of profiles of both physical and electronic records.
 - F3.8.6. The EDRMS should search records profiles regardless of the location (e.g., online or off-line) or scheduling status (e.g., active or semi-active) of the records. (Based on MoReq 8.1.19)

- F3.8.7. In the case of files, the EDRMS should present seamless functionality across searches for electronic files, hybrid files and physical files. (Based on MoReq 8.1.3)
- F3.8.8. The EDRMS should allow the user to set up a single search request with combinations of metadata and/or record content. (Based on MoReq 8.1.6)
- F3.8.9. The EDRMS should provide searching tools that cover the following techniques:
- F3.8.9.1. free text searching of combinations of record and file metadata elements and record content;
- F3.8.9.2. Boolean searching of metadata elements. (Based on MoReq 8.1.8)
- F3.8.10. The EDRMS should provide concept searching by the use of a thesaurus incorporated as an on-line index. (Based on MoReq 8.1.10)
- F3.8.11. The EDRMS should provide for “wild card” searching of metadata that allows for forward, backward and embedded expansion. (Based on MoReq 8.1.11)
- F3.8.12. The EDRMS should provide word proximity searching that can specify that a word has to appear within a given distance of another word in the record to qualify as a hit. (Based on MoReq 8.1.12)
- F3.8.13. The EDRMS should provide browsing mechanisms that provides graphical or other display browsing techniques at the classification, file/volume and records levels (including selection, retrieval and display of electronic files and their contents). (Based on MoReq 8.1.13)
- F3.8.14. The EDRMS should allow users to save and re-use queries. (Based on MoReq 8.1.20)
- F3.8.15. The EDRMS should allow users to refine (i.e., narrow) searches. (Based on MoReq 8.1.21)
- F3.8.16. The EDRMS should allow the use of named time intervals in search requests, e.g., “last week”, “this month”. (Based on MoReq 8.1.22)
- F3.8.17. The EDRMS should provide relevance ranking of the search results. (Based on MoReq 8.1.25)
- F3.8.18. When viewing or working with a record or aggregation (e.g., file or class) of records, whether as the result of a search or not, a user should be able to use EDRMS features to find information about the next-higher level of aggregation of records easily and without leaving or closing the record. (Based on MoReq 8.1.27)

For example, when reading a record, the user should be able to find out what volume and file it is in; if viewing file metadata, the user should be able to find out information about the primary-secondary in which it is located.

Display/Retrieval

An EDRMS may contain records with different formats and structures. The user requires generic viewing facilities that will accommodate rendering (displaying) a range of formats.

F3.8.19. The EDRMS should render records retrieved from searches. (Based on MoReq 8.2.1).

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

F3.8.20. The EDRMS should provide display formats, configurable by users, for search results having the functions listed below. (Based on MoReq 8.1.24)

F3.8.20.1. select the order in which the search results are presented;

F3.8.20.2. specify the number of hits displayed on the screen per view from the search;

F3.8.20.3. set the maximum number of hits for a search;

F3.8.20.4. save the search results;

F3.8.20.5. choose which metadata fields are displayed in search result lists.

F3.8.21. The EDRMS should display the total number of hits from a search on the user's screen and should allow the user to then display the search results (the "hit list"), or refine his or her search criteria and issue another request. (Based on MoReq 8.1.17)

F3.8.22. The EDRMS should allow records, files etc. listed in a hit list to be selected then opened (subject to access controls) by a single click or keystroke. (Based on MoReq 8.1.18)

F3.8.23. The EDRMS should be able to search for and retrieve a complete electronic file, or file volume, and all its contents and contextual metadata, and render all, and only, those entries in the context of that file as a discrete group and in a single retrieval process. (Based on MoReq 8.1.15)

F3.8.24. The EDRMS should render records that the search request has retrieved without loading the associated application software. (Based on MoReq 8.2.2).

F3.8.25. The EDRMS should be able to render all the types of electronic records specified by the organization in a manner that preserves the information of the records (e.g., all the features of visual presentation and layout produced by the generating application package), and which renders all components of an electronic record together. (Based on MoReq 8.2.3).

F3.8.26. The EDRMS should ensure that retrieval of a hybrid file retrieves the metadata for both electronic and paper records associated with it. (Based on MoReq 10.1.6)

F3.9. Transferring Records to Another Location

Transferring records to another location implies the movement of file volumes on-site within or between ministries; it does not refer to transferring files to off-site storage facilities or to the custody of the BC Archives (for the latter, see Scheduling Management)

F3.9.1. The EDRMS should provide a tracking feature to monitor and record information about the location and movement of volumes, both electronic and physical. (Based on MoReq 4.4.1).

- F3.9.2. The tracking function should record information about movements that includes the following:
- F3.9.2.1. unique identifier of the file or records;
 - F3.9.2.2. current location as well as a user-defined number of previous locations (locations should be user-defined);
 - F3.9.2.3. date file sent/moved from location;
 - F3.9.2.4. date file received at location (for transfers);
 - F3.9.2.5. user responsible for the move (where appropriate). (Based on MoReq 4.4.2).
- F3.9.3. The EDRMS should support tracking of physical volumes by the provision of checkout, check-in and bring forward facilities, which reflect the current location of the volume. (Based on MoReq 10.1.5)
- F3.9.4. The EDRMS should support on-line requests to reserve file volumes for future sign out; e.g., user or administrator to link bring forward criteria to a record (person requesting bring forward, due date, action to be taken, etc.).
- F3.9.5. The EDRMS should handle multiple bring forwards from different sources concurrently.
- F3.9.6. The EDRMS should support volume-level location controls for physical volumes.
- F3.9.7. The EDRMS should support individual or bulk updates of location profile information.

F4. Scheduling Management

One of the primary purposes of the EDRMS is to automate the retention and disposition of electronic records and to facilitate the retention and disposition of records in traditional media. Retention periods and disposition decisions are identified in records schedules, such as *ARCS* or *ORCS*.

Requirements for establishing, maintaining, and calculating retention periods are listed in Section B.4.1. Requirements for the processes that take place at the date specified by the retention periods are described in subsequent sections.

Requirements for review and approval processes are listed in Section B.4.2, and requirements for transfer, export and destruction are listed in Section B.4.3.

F4.1. Managing Records Schedules

- F4.1.1. The EDRMS should provide a function that specifies retention schedules, calculates retention periods and eligible disposition dates, automates reporting and destruction actions, and provides integrated facilities for exporting records and metadata. (Based on MoReq 5.1.1)
- F4.1.2. Every record of a file should be governed by the retention period(s) associated with that file.

- F4.1.3. EDRMS should provide functionality to enable all components of a file to be retained and disposed of as a unit, even if volumes are maintained in different locations and/or in different media and formats, for example, “hybrid” files.
- F4.1.4. For each file, the EDRMS should:
- F4.1.4.1. automatically track retention periods that have been allocated to the file;
- F4.1.4.2. initiate the disposal process once the end of the retention period is reached. (Based on MoReq 5.1.8)
- F4.1.5. The EDRMS should be capable of associating more than one retention period with any secondary of the classification scheme.

For example, each secondary in ARCS/ORCS is associated with two retention periods: one for the office of primary responsibility (OPR) and one for the non-office of primary responsibility (non-OPR). In addition, there may be a special schedule (such as the Executive Records Schedule) that is associated with an organizational unit or particular category of record that will override the retention periods defined in ARCS/ORCS.

- F4.1.6. The EDRMS should allow organization units to use one or more schedules simultaneously (for example, ARCS and one or more ORCS).
- F4.1.7. The EDRMS should allow authorized users to change or amend any retention period allocated to any file at any point in the life of the file. (Based on MoReq 5.1.15)
- F4.1.8. EDRMS should require determination of a file’s OPR status when the file is classified.
- F4.1.9. The Administrator should have the option to restrict the choice of OPR or non-OPR retention periods for specified secondaries (e.g., the Payroll office will have only the OPR option for Employee Pay Files, while all other offices will have only the non-OPR option).
- F4.1.10. EDRMS should allow the Administrator to designate an org unit as governed by a special schedule or defining an aggregation of files as governed by a special schedule, regardless of classification numbers applied to file(s).
- F4.1.11. When an Administrator moves files or records between secondaries of the classification scheme, the EDRMS should optionally allow the retention period of the destination secondary to replace the existing retention period(s) applying to these records. (Based on MoReq 5.1.18)
- F4.1.12. The EDRMS should support reporting and analysis tools for the management of retention and disposition schedules by the Administrator, including the ability to:
- F4.1.12.1. list all retention schedules;
- F4.1.12.2. list all files to which a specified retention schedule is assigned. (Based on MoReq 5.2.8)
- F4.1.13. The EDRMS should support retention periods that are based on time (such as a calendar year or a fiscal year), trigger events (known as “superseded or obsolete” or “SO”), or time – event retentions (superseded or obsolete plus a period of time).

- F4.1.14. The EDRMS should support retention periods of time from one month to one hundred years. (Based on MoReq 5.1.12)
- F4.1.15. The EDRMS should calculate retention period for the file based on “scheduling date”. The “scheduling date” may be the date upon which a defined cycle ends (e.g., March 31), or the date upon which a trigger event occurs (e.g., Contract ends), or a decision is made (e.g., information no longer required).
- F4.1.16. The EDRMS should allow at least the following decisions for each retention period:
 - F4.1.16.1. retain indefinitely;
 - F4.1.16.2. present for review at a future date, as defined below;
 - F4.1.16.3. destroy at a future date, as defined below;
 - F4.1.16.4. transfer at a future date, as defined below. (Based on MoReq 5.1.10)
- F4.1.17. Each retention schedule should allow the retention periods to be specified for a future date, with the date being specified in at least the following ways:
 - F4.1.17.1. passage of a specified period of time after the file is opened;
 - F4.1.17.2. passage of a specified period of time after the file is closed;
 - F4.1.17.3. elapse of a specified interval since assignment of the last record to the file;
 - F4.1.17.4. elapse of a specified interval since a record was retrieved from the file;
 - F4.1.17.5. elapse of a specified interval since a specific event described in the schedule that results in a notification being sent to the EDRMS from the Administrator (rather than being detected automatically by the EDRMS). (Based on MoReq 5.1.11)

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

- F4.1.18. The EDRMS should, by default, prevent the user from adding electronic records to a closed file.
- F4.1.19. The EDRMS should permit authorized users to suspend the retention period and final disposition of a file(s). The suspension (“hold”) is applied at the file level and affects all components of the file.
 - F4.1.19.1. EDRMS should permit authorized users to lift “holds.”
 - F4.1.19.2. EDRMS should support the placing or lifting of holds on single files and/or classes of files.

F4.2. Applying Retention Periods, Including Review and Approval

The records officer is required to review and approve any transfer or disposition actions to ensure that users are using the retention schedules correctly. The EDRMS should have

functionality to assist users in determining which records are ready for transfer or disposal, and to assist records officers in reviewing the application of records schedules.

- F4.2.1. The EDRMS should support the creation of reports (“pull lists”) listing all open files that have reached the end of their active retention period and are eligible for transfer or disposition. These lists should be organized to facilitate boxing of physical files, that is, by final disposition date and final disposition action (e.g., selective/full retention or destruction).
- F4.2.2. The EDRMS should allow volumes to be transferred off-site even if they are still active.
- F4.2.3. The EDRMS should allow for closed files/volumes in off-site storage to be reactivated, or permanently removed from a box and re-entered into the active records management system.
- F4.2.4. The EDRMS should support box/container management functions, such as:
 - F4.2.4.1. calculating the eligible disposition date for the box/container based upon the file with the longest retention period in the box; or
 - F4.2.4.2. recalculating the eligible disposition date should any files be permanently removed from the box/container.
- F4.2.5. The EDRMS should allow the definition of sets of processing rules to be applied as an alerting facility to specified files, prior to initiation of the disposal process. Specific requirements should include the following:
 - F4.2.5.1. managers and Administrators should be able to review files and contents;
 - F4.2.5.2. the EDRMS should notify the Administrator of files with a given security level.
- F4.2.6. The EDRMS should be able to notify the Administrator regularly of all retention periods that will come into force in a specified period of time, and provide quantitative reports on the volumes and types of records. (Based on MoReq 5.2.1)
- F4.2.7. The Administrator should be able to specify the frequency of a retention period report, the information reported and highlighting exceptions such as disposal overdue. (Based on MoReq 5.2.2)
- F4.2.8. The EDRMS should support the review process by presenting electronic files to be reviewed, with their metadata and retention schedule information (the reason), in a manner which allows the reviewer to browse (i.e., navigate and study) the file contents and/or metadata efficiently. (Based on MoReq 5.2.3)

In practice, this implies features for navigating forward, back etc. within and between files, and from/to the metadata for files and records.

- F4.2.9. The EDRMS should alert the Administrator if an electronic file/record that is due for destruction is referred to in a link from another file/record; and should pause the destruction process to allow the following remedial actions to be taken:

- F4.2.9.1. confirmation by the Administrator to proceed with or cancel the process; and
- F4.2.9.2. the generation of a report detailing the files or records and all references or links for which it is a destination. (Based on MoReq 5.2.4)
- F4.2.10. The EDRMS should allow the reviewer to take at least any of the following actions for each file during review:
 - F4.2.10.1. mark the file for deletion;
 - F4.2.10.2. mark the file for transfer;
 - F4.2.10.3. change the retention period (or assign a different schedule) so that the file is retained and re-reviewed at a later date. (Based on MoReq 5.2.5)
- F4.2.11. The EDRMS should allow the reviewer to enter comments into the file's metadata to record the reasons for the review decisions. (Based on MoReq 5.2.6)
- F4.2.12. The EDRMS should alert the Administrator to files due for disposal before implementing disposal actions; and on confirmation from the Administrator the EDRMS should be capable of initiating the disposal actions. (Based on MoReq 5.2.7)
- F4.2.13. The EDRMS should store in the audit trail all decisions taken by the reviewer during reviews. (Based on MoReq 5.2.9)
- F4.2.14. The EDRMS should provide, or support the ability to interface with, a workflow facility to support the scheduling, review and export/transfer process, by tracking:
 - F4.2.14.1. progress/status of the review, such as awaiting or in-progress, details of reviewer and date;
 - F4.2.14.2. records awaiting disposal as a result of a review decision;
 - F4.2.14.3. progress of the transfer process. (Based on MoReq 5.2.10)
- F4.2.15. The EDRMS should be able to accumulate statistics of review decisions in a given period and provide tabular and graphical reports on the activity. (Based on MoReq 5.2.11)

F4.3. Disposition and Transfer/Export

Disposition refers to the destruction of records or the transfer of *the legal custody* (ownership) of the records to an agency external to government (i.e., their alienation from the Crown provincial) or to the BC Archives.

Transfer/export indicates transfer of physical records to off-site storage facilities and/or transfer or export of electronic records to external systems. For example, it may be necessary to export file/volumes to another EDRMS and it will be necessary to export transfer/export selected file/volumes of records to the BC Archives for permanent preservation.

Transfer/export will include both record content and descriptive material relating to record context, such as file structure, file/volume and record metadata. To support the process of review and preparation for transfer, it may be necessary to add free-text annotations as metadata at the file/volume level, such as: the primary/secondary classifications to be used

for records transferred to a new organisation; the reasons for transfer/disposition decisions; accession numbers or other data supplied by BC Archives for use in archival finding aids; etc.

Disposition

- F4.3.1. The EDRMS should permit disposition to be processed for files covered by approved records schedules only (i.e., not for files linked to draft schedules).
- F4.3.2. All volumes/records associated with a file should be disposed before the disposition of the file is confirmed by the EDRMS.
- F4.3.3. The EDRMS should provide orderly processes supporting the application of a records schedule's disposition instructions, including processes for:
 - F4.3.3.1. review of the electronic file/volume and contents;
 - F4.3.3.2. export of the electronic file/volume and contents for permanent preservation;
 - F4.3.3.3. destruction of the electronic file/volume and contents. (Based on PRO, A.3.13)
- F4.3.4. The EDRMS should require approval by a Records Officer or authorized delegate before permitting or performing destruction of any record.
- F4.3.5. The EDRMS should allow individual and batch destruction action upon authorized approval and confirmation.
- F4.3.6. The EDRMS should enable the total destruction of files and records that are stored on rewritable media, by completely obliterating them so that they cannot be restored by use of specialist data recovery facilities. (Based on MoReq 5.3.13)
- F4.3.7. If records are stored on write-once media, the EDRMS should provide facilities to prevent access to them so that they cannot be restored by normal use of the EDRMS or by standard operating system utilities. (Based on MoReq 5.3.14)
- F4.3.8. The EDRMS should support documentation of on-site records destruction of both electronic and physical records (i.e., destruction of records *not* stored in off-site storage facilities managed by BC Archives). This documentation should include lists of files/records eligible for destruction, reports documenting authorizations, and date of completed destruction.

Transfer/Export (e.g., to other EDRMS or to BC Archives)

- F4.3.9. The EDRMS should provide a well-managed process to transfer records to another system or to a third party organization. (Based on MoReq 5.3.1)
- F4.3.10. The EDRMS should be able to support the flagging of electronic files/volumes and groups of files/volumes for export to another EDRMS, or for transfer to the BC Archives for permanent preservation. (Based on PRO A.3.25)
- F4.3.11. The EDRMS should be able to identify and list electronic files/volumes marked for permanent preservation as their disposal schedules come into force. (Based on PRO A.3.26)

- F4.3.12. The EDRMS should provide the ability to:
- F4.3.12.1. add user-defined metadata elements (e.g., elements required for archival management purposes) to electronic file/volumes selected for transfer;
 - F4.3.12.2. sort electronic files/volumes selected for transfer into ordered lists according to user-defined metadata elements;
 - F4.3.12.3. generate user-defined forms to describe electronic files/volumes that are being exported or transferred. (Based on MoReq 5.3.11; PRO A.3.42)
- F4.3.13. Where an EDRMS does not support the addition of metadata to electronic files/volumes selected for export or transfer, and the sorting of files/volumes into ordered lists, it should interface with an appropriate package (for example a report management package) for this purpose. (Based on PRO A.3.29)
- F4.3.14. The EDRMS should support transfer of electronic records to BC Archives in both native and non-proprietary formats (XML preferred).
- F4.3.15. The EDRMS should ensure profile information is available for files transferred to the legal custody of the BC Archives is available in standard, non-proprietary format (XML preferred).
- F4.3.16. The EDRMS should provide a utility or conversion tool to support the rendition of records marked for transfer or export into specified transfer format(s), e.g.:
- F4.3.16.1. extensible mark-up language (XML);
 - F4.3.16.2. single page TIFF images (TIFF ver 6.0 with lossless compression);
 - F4.3.16.3. Delimited (e.g., Comma Separated Variable Length). (Based on MoReq 5.3.5)
- F4.3.17. Where an EDRMS does not support the rendering of records and files/volumes marked for transfer into an approved transfer format, it should interface with an appropriate package or conversion utility for this purpose. (Based on PRO A.3.30)
- F4.3.18. Whenever the EDRMS transfers the contents of any primary classification, file or volume, the transfer should include:
- F4.3.18.1. all files in a primary class (for classes);
 - F4.3.18.2. all volumes below the file in the hierarchy (for files);
 - F4.3.18.3. all records in all these files and volumes;
 - F4.3.18.4. All metadata associated with the files, records and volumes. (Based on MoReq 5.3.2)

- F4.3.19. The EDRMS should be able to export a whole electronic file or entire set of files within a primary classification in one sequence of operations, such that:
- F4.3.19.1. the content and appearance of the electronic records are not degraded;
 - F4.3.19.2. all components of an electronic record, when the record consists of more than one component, are exported as an integral unit; for example, an e-mail message with associated file attachment;
 - F4.3.19.3. all metadata associated with an electronic record is linked to the record to which it belongs;
 - F4.3.19.4. all electronic records within a specific file/volume remain associated with that file/volume;
 - F4.3.19.5. all electronic file/volume metadata is exported and remains associated with that electronic file/volume. (Based on MoReq 5.3.3; PRO A.3.27)
- F4.3.20. The EDRMS should be able to export groups of electronic files/volumes, or an entire primary of the classification scheme in one sequence of operations, such that all conditions of the above requirement are met, and:
- F4.3.20.1. the relative location of each file/volume in the electronic file plan structure is maintained, so that the file/volume structure can be reconstructed;
 - F4.3.20.2. all file/volume metadata at higher points in the hierarchy is retained with that file/volume. (Based on MoReq 5.3.8; PRO A.3.40)
- F4.3.21. Whenever the EDRMS transfers or exports records, the EDRMS must be able to include a copy of all the audit trail data associated with the files, volumes and records being transferred. (Based on MoReq 5.3.4)
- F4.3.22. The EDRMS should be able to export multiple entries, where an electronic file/volume to be exported contains a pointer rather than the physical record; at a minimum, by achieving this effect through duplication of records to be exported. (Based on PRO A.3.28)
- F4.3.23. The EDRMS should be able to export and transfer multiple entries (i.e., links between a physical record and its entry in more than one file/volume) without duplication of records. (Based on PRO A.3.39)
- F4.3.24. The EDRMS should produce a report detailing any failure during a transfer, export or deletion. The report should identify any records destined for transfer which have generated processing errors, and any files or records and associated metadata which are not successfully transferred, exported or deleted. (Based on MoReq 5.3.6)
- F4.3.25. The EDRMS should retain all electronic files that have been transferred, at least until confirmation of a successful transfer process. (Based on MoReq 5.3.7)
- F4.3.26. Where hybrid files are to be transferred, exported or destroyed, the EDRMS should require the Administrator to confirm that the paper part of the same files has been transferred, exported or destroyed before transferring, exporting or destroying the electronic part. (Based on MoReq 5.3.9)

- F4.3.27. The EDRMS should allow records to be transferred or exported more than once. (Based on MoReq 5.3.17)
- F4.3.28. The EDRMS should have the ability to retain metadata for files and records that have been destroyed or transferred. (Based on MoReq 5.3.15)
- F4.3.29. The EDRMS should allow the Administrator to specify a subset of file metadata that will be retained for files destroyed, transferred out or moved offline, which can be indexed and retrieved alongside metadata for existing records, to indicate the absence of sought items. (Based on MoReq 5.3.16; PRO A.3.43)
- F4.3.30. The EDRMS should support the selection and export of electronic record and file/volume metadata, independently from record content, in a form suitable for migration to a Web-based environment. (Based on PRO A.3.38)]

F5. Preservation and Ongoing Access

- F5.1.1. The EDRMS should be capable of supporting the preservation of records beyond the anticipated life cycle of their source applications, by enabling the following preservation metadata to be captured in the records profiles:
 - F5.1.1.1. file names;
 - F5.1.1.2. hardware dependencies;
 - F5.1.1.3. operating system dependencies;
 - F5.1.1.4. application software dependencies (application names and versions);
 - F5.1.1.5. file formats;
 - F5.1.1.6. resolution;
 - F5.1.1.7. compression algorithm version and parameters;
 - F5.1.1.8. encoding scheme;
 - F5.1.1.9. rendition information. (Based on MoReq 12.7.13)
- F5.1.2. The EDRMS should be able to retrieve records throughout their required retention periods by utilizing storage media with appropriate long-term life expectancy ratings and enabling the replacement of media, hardware, and software components to address component obsolescence. (Based on AIIM, p.8)
- F5.1.3. The EDRMS should maintain internal integrity (relational integrity or otherwise) at all times, regardless of maintenance activities; other user actions; failure of system components. (Based on MoReq 3.4.12)
- F5.1.4. The EDRMS should include features for the automated periodic comparison of copies of information, and the replacement of any copy found to be faulty, to guard against media degradation. (Based on MoReq 11.7.2)
- F5.1.5. The EDRMS should allow the bulk conversion of records (with their metadata and audit trail information) to other media and/or systems in line with the standards relevant for the formats in use. (Based on MoReq 11.7.3)

- F5.1.6. The EDRMS supplier should have a demonstrable program in place for upgrades to the EDRMS technology base that allows for the existing information to continue to be accessed without changes to the content. (Based on MoReq 11.7.4)
- F5.1.7. The EDRMS should use only widely accepted standards that are the subject of open and publicly available specifications for encoding, storage and database structures. (Based on MoReq 11.7.5)
- F5.1.8. If the EDRMS uses any proprietary encoding or storage or database structures, these should be fully documented, with the documentation being available to the Administrator. (Based on MoReq 11.7.6)

F6. Security

Security requirements include the ability to protect records from unauthorized destruction; define security categories for records; control user access to records and to system functions; maintain audit trails of system activities, and provide backup and recovery controls, including recovery of vital records.

F6.1. Deletion of Records

- F6.1.1. The EDRMS should allow a default or option that prevents any record, once captured, from being deleted or moved by any Administrator or user. This means that any requirement for an Administrator to consider a record as “deleted” or “re-located” means that the record is marked appropriately; and in the case of re-location, a copy or pointer is inserted at the new location. *This requirement does not affect transfer or destruction of records in accordance with a retention schedule.* (Based on MoReq 9.3.1)
- F6.1.2. The EDRMS should allow an option at configuration time, as an alternative to the deletion option specified above, that “deletion” of a record is implemented as destruction of that record. (Based on MoReq 9.3.2)
- F6.1.3. If the EDRMS is configured so that “deletion” of a record is implemented as destruction of that record, the EDRMS should, in the event of any such deletion:
 - F6.1.3.1. record the deletion comprehensively in the audit trail;
 - F6.1.3.2. produce an exception report for the Administrator;
 - F6.1.3.3. delete the entire contents of a file or volume when it is deleted;
 - F6.1.3.4. ensure that no documents are deleted if their deletion would result in a change to another record (for example if a document forms a part of two records - one of which is being deleted);
 - F6.1.3.5. highlight to the Administrator any links from another file, or record to a file or volume that is about to be deleted, requesting confirmation before completing the deletion;
 - F6.1.3.6. maintain complete integrity of the metadata at all times. (Based on MoReq 9.3.7)

F6.2. Records Security Categories

- F6.2.1. The Administrator should be able to change the security category of individual records. (Based on MoReq 9.3.3)
- F6.2.2. The Administrator should be able to change the security category of all records in a file or class in one operation; the EDRMS should provide a warning if any records are having their security category lowered, and await confirmation before completing the operation. (Based on MoReq 9.3.4)
- F6.2.3. The EDRMS should record full details of any change to security category in the metadata of the record, volume or file affected. (Based on MoReq 9.3.6)
- F6.2.4. The EDRMS should record the date on which a security classification should be reviewed. (Based on MoReq 12.5.19)
- F6.2.5. Where files have security categories, the EDRMS should ensure that a hybrid physical file is allocated the same security category as an associated hybrid electronic file. (Based on MoReq 10.1.7)
- F6.2.6. The EDRMS should include the ability to control access to records based on intellectual property restrictions, and generate charging data. (Based on MoReq 8.1.29)

F6.3. User Access/Authentication

- F6.3.1. The EDRMS should integrate with security protocols, user authentication models and access control methods commonly deployed in similar government / industry environments; i.e., should:
 - F6.3.1.1. integrate with LDAP and Windows 2000 Active Directory;
 - F6.3.1.2. provide mechanisms to deal with document authentication, non-repudiation, integrity and privacy;
 - F6.3.1.3. provide methods to manage changing security policies.
- F6.3.2. The EDRMS should integrate with common authentication services for access to existing and emerging document-related services. It should do this by:
 - F6.3.2.1. incorporating BC government security tables established through the BCGOV ID assigned to government employees and authorized personnel;
 - F6.3.2.2. provide a login that uses or is unified with that of the BC government LAN;
 - F6.3.2.3. allow users and groups to be imported from the operating system.
- F6.3.3. The EDRMS should allow the Administrator to limit access to records, files and metadata to specified users or user groups. (Based on MoReq 4.1.1)
- F6.3.4. The EDRMS should allow the Administrator to attach to the user profile attributes that determine the features, metadata fields, records or files to which the user has access. The attributes of the profile should:

- F6.3.4.1. prohibit access to the EDRMS without an accepted authentication mechanism attributed to the user profile;
- F6.3.4.2. restrict user access to specific files or records;
- F6.3.4.3. restrict user access to specific parts of the classification scheme;
- F6.3.4.4. restrict user access according to the user's security clearance;
- F6.3.4.5. restrict user access to particular features (e.g., create, read, up-date and/or delete specific metadata fields; change records profile metadata, open/close files/volumes, register records, perform scheduling activities, dispose of physical and electronic records, etc);
- F6.3.4.6. deny access after a specified date;
- F6.3.4.7. allocate users to a group or groups. (Based on MoReq 4.1.2)
- F6.3.5. The Administrator should be able to change any user-entered metadata element. Information about any such change should be stored in the audit trail
- F6.3.6. The EDRMS should be able to provide the same control functions for roles as for users. (Based on MoReq 4.1.3)

This feature allows administrators to manage and maintain a limited set of role access rights rather than a larger number of individual users. Examples of roles might include Records Officer, Records Clerk, Database Administrator.

- F6.3.7. The EDRMS should be able to set up groups of users that are associated with a set of files or records. (Based on MoReq 4.1.4)

Examples of groups might be Personnel, project working groups.

- F6.3.8. The EDRMS should allow a user to be a member of more than one group. (Based on MoReq 4.1.5)
- F6.3.9. The EDRMS should allow only Administrators to set up user profiles and allocate users to groups. (Based on MoReq 4.1.6)
- F6.3.10. The EDRMS should allow a user to stipulate which other users or groups can access records for which the user is responsible. (Based on MoReq 4.1.7)
- F6.3.11. The EDRMS should 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 Administrators. (Based on MoReq 4.1.8)
- F6.3.12. The EDRMS should support establishment of permissions that control scope of user searches (e.g., within specified organizational units; across specified organizational units; entire ministry).
- F6.3.13. The EDRMS should not display record/volume/file information unless the user has access permissions for information. (Based on MoReq 8.1.28)

- F6.3.14. If a user requests access to, or searches for, a record, volume or file which he or she does not have the right to access, the EDRMS should provide one of the following responses (selectable at configuration time):
- F6.3.14.1. display title and metadata;
 - F6.3.14.2. display the existence of a file or record (i.e., display its file or record number) but not its title or other metadata;
 - F6.3.14.3. do not display any record information or indicate its existence in any way. (Based on MoReq 4.1.9)
- F6.3.15. If a user performs a full text search, the EDRMS should never include in the search result list any record that the user does not have the right to access. (Based on MoReq 4.1.10)
- F6.3.16. If the EDRMS allows users to make unauthorized attempts to access files, volumes or records, it should log these in the audit trail. (Based on MoReq 4.1.11)

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

- F6.3.17. The EDRMS should provide the capability to limit users' access to parts of the file list (as specified at configuration time). (Based on MoReq 4.1.12)
- F6.3.18. The EDRMS should include features to control and record access to physical files, including controls based on security category, which are comparable to the features for electronic files. (Based on MoReq 10.1.8)

F6.4. Audit

- F6.4.1. The EDRMS should create an unalterable audit trail capable of automatically capturing and storing information about:
- F6.4.1.1. all the actions that are taken upon an electronic record, electronic file or classification scheme;
 - F6.4.1.2. the user initiating and or carrying out the action;
 - F6.4.1.3. the date and time of the event. (Based on MoReq 4.2.1)

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

- F6.4.2. Once the audit trail functionality has been activated, the EDRMS should track events without manual intervention, and store in the audit trail information about them. (Based on MoReq 4.2.2)
- F6.4.3. The EDRMS should maintain the audit trail for as long as required, which will be at least for the life of the electronic records or electronic files to which it refers. (Based on MoReq 4.2.3)
- F6.4.4. The EDRMS should provide an audit trail of all changes made to:

- F6.4.4.1. groups of electronic files;
- F6.4.4.2. individual electronic files;
- F6.4.4.3. electronic volumes;
- F6.4.4.4. electronic records;
- F6.4.4.5. electronic documents;
- F6.4.4.6. metadata associated with any of the above. (Based on MoReq 4.2.4)
- F6.4.5. The EDRMS should provide an audit trail of all changes made to administrative parameters. (Based on MoReq 4.2.5)

For example, if the Administrator changes a user's access rights.

- F6.4.6. The EDRMS should be capable of capturing and storing in the audit trail information about the following actions:
 - F6.4.6.1. the date and time of capture of all electronic records;
 - F6.4.6.2. re-classification of an electronic record in another electronic volume;
 - F6.4.6.3. re-classification of an electronic file within the classification scheme;
 - F6.4.6.4. any change to the retention schedule of an electronic file;
 - F6.4.6.5. any change made to any metadata associated with classes, electronic files or electronic records;
 - F6.4.6.6. date and time of creation, amendment and deletion of metadata;
 - F6.4.6.7. changes made to the access privileges affecting an electronic file, electronic record or user;
 - F6.4.6.8. export or transfer actions carried out on an electronic file;
 - F6.4.6.9. date and time of a rendition;
 - F6.4.6.10. deletion / destruction actions on an electronic file or electronic record. (Based on MoReq 4.2.6)
- F6.4.7. The EDRMS should allow the audit trail facility to be configurable by the Administrator so that he can select the functions for which information is automatically stored; and the EDRMS should ensure that this selection and all changes to it are stored in the audit trail. (Based on MoReq 4.2.7)
- F6.4.8. The EDRMS should ensure that audit trail data is available for inspection on request, so that a specific event can be identified and all related data made accessible, and that this can be achieved by authorized external personnel who have little or no familiarity with the system. (Based on MoReq 4.2.8)

- F6.4.9. The EDRMS should be able to export audit trails for specified electronic records, electronic files and groups of files (without affecting the audit trail stored by the EDRMS). (Based on MoReq 4.2.9)
- F6.4.10. The EDRMS should be able to capture and store violations (i.e., a user's attempts to access a record, volume or file to which he or she is denied access), and (where violations can validly be attempted) attempted violations, of access control mechanisms. (Based on MoReq 4.2.10)

F6.5. Backup and Recovery

- F6.5.1. The EDRMS should provide automated backup and recovery procedures that allow for the regular backup of all or selected classification levels (e.g., primaries, secondaries), files, records, metadata and administrative attributes of the EDRMS repository. (Based on MoReq 4.3.1)
- F6.5.2. The EDRMS should allow the Administrator to schedule backup routines by:
 - F6.5.2.1. specifying the frequency of backup;
 - F6.5.2.2. selecting classification levels (e.g., primaries, secondaries; files or records) to be backed up;
 - F6.5.2.3. selecting storage media, system or location for the backup (e.g., off-line storage, separate system, remote site). (Based on MoReq 4.3.2)

F6.6. Vital Records

- F6.6.1. The EDRMS should allow users to indicate that selected records are considered to be "vital records". (Based on MoReq 4.3.6)
- F6.6.2. The EDRMS should allow vital records and other records to be restored in distinct operations (e.g., it should be possible to recover vital records without having to achieve full recovery of all records in the same repository). (Based on MoReq 4.3.7)

F7. Printing and Reports

F7.1. Printing

- F7.1.1. The EDRMS should provide the user with flexible ways of printing records and their relevant metadata, including the ability to print a record(s) with metadata specified by the user. (Based on MoReq 8.3.1).
- F7.1.2. The EDRMS should allow the printing of metadata for a file. (Based on MoReq 8.3.2).
- F7.1.3. The EDRMS should allow the user to be able to print out a summary list of selected records (e.g., the contents of a file), consisting of a user-specified subset of metadata elements (e.g., Title, Author, Creation date) for each record. (Based on MoReq 8.3.4).
- F7.1.4. The EDRMS should allow the Administrator to specify that all printouts of records have selected metadata elements appended to them, e.g., title, registration number, date, security category. (Based on MoReq 8.3.5).
- F7.1.5. The EDRMS should allow users to print search result hit lists. (Based on MoReq 8.3.6).
- F7.1.6. The EDRMS should allow users to print search parameters.

- F7.1.7. The EDRMS should allow the Administrator to print any and all administrative parameters. (Based on MoReq 8.3.7).
- F7.1.8. The EDRMS should allow Administrators to print a thesaurus (e.g., schema of authorized/controlled indexing terms). (Based on MoReq 8.3.9)
- F7.1.9. The EDRMS should allow Administrators to print file lists. (Based on MoReq 8.3.11)
- F7.1.10. The EDRMS should allow Administrators to print audit trails. (Based on MoReq 8.3.12).
- F7.1.11. The EDRMS should be able to print (at minimum) all common forms of BC government office records (e.g., MS Outlook and MS Office records). Printing should:
 - F7.1.11.1. preserve the layout produced by the generating application;
 - F7.1.11.2. include all (printable) components of the electronic record. (Based on MoReq 8.3.13)

F7.2. Reports

- F7.2.1. The EDRMS should:
 - F7.2.1.1. provide “canned” (pre-defined) reports;
 - F7.2.1.2. support or link to an external application to support ad-hoc reports
- F7.2.2. The EDRMS should provide the capability to produce/export reports in common and preferably non-proprietary electronic formats, including:
 - F7.2.2.1. XML;
 - F7.2.2.2. PDF.
- F7.2.3. The EDRMS should support reports based on user criteria in order to perform location management functions to specified files/volumes, (i.e., inventories of holdings, box content file lists, audit reports, security reports, etc).
- F7.2.4. The EDRMS should support eligibility reports (pull lists) based on user criteria to perform scheduling management actions, and organize reports as required by users. These reports should:
 - F7.2.4.1. identify missing or charged out files and/or volumes;
 - F7.2.4.2. note “holds” (or not bring up “holds”) – all files should be eligible;
 - F7.2.4.3. arrange information in a way that facilitates the placement of volumes in boxes by final disposition date and final disposition type (like with like). The pull lists are based on profile data and classification data.
- F7.2.5. The EDRMS should be able to produce standard box content file lists showing for each file/volume at minimum: the schedule, primary, secondary, file and volume numbers; primary, secondary and file titles/codes; OPR designation; and the earliest/latest record dates.

- F7.2.6. The EDRMS should support management reports (statistics, usage, errors, etc) for records officer reporting.
- F7.2.7. The EDRMS should support audit reports based on security parameters, use, access etc.
- F7.2.8. The EDRMS should be able to produce a report listing of files and volumes, structured to reflect the classification scheme, for all or part of the classification scheme. (Based on MoReq 9.2.4)
- F7.2.9. The EDRMS should include features for sorting and selecting report information. (Based on MoReq 9.2.5)
- F7.2.10. The EDRMS should include features for totaling and summarizing report information. (Based on MoReq 9.2.6)
- F7.2.11. The EDRMS should allow authorized users to request regular periodic reports and one-off reports. (Based on MoReq 9.2.7)

F7.3. Labelling

- F7.3.1. EDRMS should be able to generate labels for the components of a file (e.g., file folders, filebacks, binders, tapes, and other physical containers for records).
- F7.3.2. The EDRMS should support:
 - F7.3.2.1. the printing and recognition of bar codes; and/or
 - F7.3.2.2. other tracking systems (e.g., to automate the data entry for tracking physical box/file movements). (Based on MoReq 10.1.9)
- F7.3.3. An authorized user (e.g. MRO) should be able to specify content of a label (fields that will print).
- F7.3.4. A user should able to specify number of labels to print (single, multiple, or batch).
- F7.3.5. A user should be able to generate different formats for file labels and volume labels

F8. Administrative Functions

F8.1. General Systems Administration

- F8.1.1. The EDRMS should allow Administrators, in a controlled manner and without undue effort, to retrieve, display and re-configure systems parameters and choices made at configuration time—for example, on elements to be indexed—and to re-allocate users and functions to user roles. (Based on MoReq 9.1.1).
- F8.1.2. The EDRMS should provide back-up facilities, and features to rebuild forward using restored back-ups and audit trails, while retaining system integrity. (Based on MoReq 9.1.2)

In other words, the EDRMS should include functionality to recreate the records and metadata to a known status, using a combination of restored back-ups and audit trails.

- F8.1.3. The EDRMS should provide recovery and rollback facilities in the case of system failure or update error, and should notify Administrators of the results. (Based on MoReq 9.1.3)

In other words, the EDRMS should allow Administrators to “undo” a series of transactions until a status of assured database integrity is reached. This is only required when error conditions arise.

- F8.1.4. The EDRMS should 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. (Based on MoReq 9.1.4).
- F8.1.5. The EDRMS should monitor error rates occurring on storage media, and report to the Administrator any medium or device on which the error rate is exceeding a parameter set at configuration time. (Based on MoReq 9.1.5)

This particularly applies to optical media.

F8.2. Administrative Reports

- F8.2.1. The EDRMS should provide flexible reporting facilities for the Administrator. They should include, at a minimum, the ability to report the following items.
 - F8.2.1.1. numbers of files, volumes and records;
 - F8.2.1.2. transaction statistics for files, volumes and records;
 - F8.2.1.3. activity reports by user. (Based on MoReq 9.2.1)
- F8.2.2. The EDRMS should allow Administrators to enquire on and produce reports on the audit trail. These reports should include, at a minimum, reporting based on items listed below:
 - F8.2.2.1. classification elements (primaries and secondaries);
 - F8.2.2.2. files;
 - F8.2.2.3. volumes;
 - F8.2.2.4. records;
 - F8.2.2.5. users;
 - F8.2.2.6. time periods. (Based on MoReq 9.2.2)
- F8.2.3. The EDRMS should allow Administrators to enquire on and produce audit trail reports based on the items listed below:
 - F8.2.3.1. security categories;
 - F8.2.3.2. user groups;
 - F8.2.3.3. other metadata. (Based on MoReq 9.2.3)
- F8.2.4. The EDRMS should allow Administrators to restrict users’ access to selected reports. (Based on MoReq 9.2.8)

F9. Document Management

This section provides requirements for the document management portion of the Proponent's integrated EDRMS solution. The document management portion of the EDRMS should provide a robust enterprise infrastructure for building future document-centric business applications.

F9.1. General Requirements

- F9.1.1. The document management portion of the EDRMS should fully support broadly available document services used to manage documents independent of the applications used to create them. These services should include the ability to:
 - F9.1.1.1. check documents "in" and "out" of information repositories;
 - F9.1.1.2. automatically update document version numbers whenever a previously "checked-out" document is modified and returned to the document repository;
 - F9.1.1.3. prevent more than one person from checking documents out for modification;
 - F9.1.1.4. utilize a security model ensuring that only authorized users can perform the above functions;
 - F9.1.1.5. provide full lifecycle management capabilities for tracking of document versions /statuses;
 - F9.1.1.6. provide full text searching capabilities in accordance with Common Command Language(CCL) (ISO 8777);
 - F9.1.1.7. manage compound (virtual) documents. (Based on AIIM, pp. 13, 21)
- F9.1.2. The document management portion of the EDRMS should support Enterprise Report Management (ERM) functionality. This is also known as Computer Output to Laser Disk (COLD) functionality.
- F9.1.3. The document management portion EDRMS should provide the ability to manage annotations. In the case of CAD documents, this can be taken to mean the proposed system should provide the ability to manage redline mark ups as separate documents. These annotations should be controlled by a security mechanism that can control which users have access to annotations independently of any access controls documents to which they apply.
- F9.1.4. The document management portion of the EDRMS should provide the ability to manage the components of a document. In the case of CAD documents, which often consist of "vector" components set against a "raster" background, all components of vector/raster hybrids should be associated for ease of search and retrieval.
- F9.1.5. The document management portion of the EDRMS should provide the ability to automatically generate renditions of documents. This means that it should be possible for a document in one file format to have a rendition in another format associated with it.

The proposed system should be able to determine and dispatch the most appropriate rendition when a user requests a rendered document.

- F9.1.6. The document management portion of the EDRMS should provide the ability to define (and redefine) document types and associated metadata. This functionality should be similar to, yet independent of, the profiling metadata of the records management portion of the EDRMS.
- F9.1.7. The document management portion of the EDRMS should provide a security mechanism that has the following characteristics;
- F9.1.7.1. security is set at the level of the document;
- F9.1.7.2. security is managed through Access Control Lists (ACLs);
- F9.1.7.3. document management security integrates with the records management security mechanisms.

F9.2. Interaction with RM Functions

Note: One intent of the following requirements is to ensure that future technology components brought into the integrated system will not defeat the records management functions of the EDRMS.

- F9.2.1. The document system should be able to access the Records Management metadata, which should be protected from modifications through the document management system.
- F9.2.2. The document management portion of the EDRMS should be able to capture automatically electronic documents arising in the course of business and pass them to the EDRMS records registration process. (Based on MoReq 10.3.1)
- F9.2.3. The document management portion of the EDRMS should be able to capture an electronic record in one process OR register an electronic document that can be captured as a record at a later time. (Based on MoReq 10.3.2)
- F9.2.4. The document management portion of the EDRMS should allow users to register a document from within the document management client software or an application integrated with the EDRMS, such as the applications of the Microsoft Office Suite. (Based on MoReq 10.3.3)
- F9.2.5. When users are in the document management portion of the EDRMS or in an application integrated with the EDRMS, they should be able to switch adroitly to and from the records management portion of the EDRMS in order to register a document as a record. (Based on MoReq 10.3.4)
- F9.2.6. The document management portion of the EDRMS should support automated acquisition of metadata elements and allow additional metadata elements to be completed by the user. (Based on MoReq 10.3.5)
- F9.2.7. The document management portion of the EDRMS should be able to manage electronic documents (not registered as records) in the context of the same classification scheme and access control mechanisms as electronic records. (Based on MoReq 10.3.7)

- F9.2.8. The document management portion of the EDRMS should be able to access the ARCS/ORCS classification system. (Based on MoReq 10.3.8)
- F9.2.9. The document management portion of the Proponent's solution should have capabilities for managing versions of electronic documents as separate but related entities. It should provide capabilities for pruning unwanted versions and provide tools to automate the management of version histories. (Based on MoReq 10.3.9)
- F9.2.10. The document management portion of the EDRMS should be configurable to restrict users to viewing either the latest version of a document, or selected versions of a document. or versions that have been captured as records. Access to this functionality should be in accordance with set security policies. (Based on MoReq 10.3.10)
- F9.2.11. The document management portion of the EDRMS should be able to integrate with related software, including image processing and scanning systems, and workflow systems, without relinquishing control of any existing electronic records. (Based on MoReq 10.3.11)
- F9.2.12. The document management portion of the EDRMS should be able to copy the content of an electronic record, in order to create a new electronic document, while ensuring the retention of the original record remains intact. (Based on MoReq 10.3.12)

F10. Other Functionality

F10.1. Workflow

- F10.1.1. The document management portion of the EDRMS should provide or link to an engine for building ad hoc or collaborative workflows that meet the standards set out by the Workflow Management Coalition (WfMC) for document-centric workflows, including support for WfMC Application Programming Interfaces (API's).
- F10.1.2. The EDRMS should provide or support the construction of workflows for records scheduling, review and export/transfer processes; e.g., by enabling the tracking of:
 - F10.1.2.1. progress of the review - awaiting, in progress, reviewer details and date;
 - F10.1.2.2. awaiting disposal as a result of a review decision;
 - F10.1.2.3. progress of records transfer processes.
- F10.1.3. The EDRMS should support workflows consisting of a number of steps, each step being (for example) movement of a record or file from one participant to another for action. (Based on MoReq 10.4.1)
- F10.1.4. The EDRMS should not practically limit the number of steps in each workflow. (Based on MoReq 10.4.2)
- F10.1.5. The EDRMS should provide a function to alert a user participant that documents records have been sent for attention and specify the action required. (Based on MoReq 10.4.3)
- F10.1.6. The EDRMS should enable a user to send e-mail messages to users to notify them of records requiring their attention. (Based on MoReq 10.4.4)
- F10.1.7. The EDRMS should allow programmed workflows to be defined and maintained by the Administrator. (Based on MoReq 10.4.5)

- F10.1.8. The EDRMS should prevent programmed workflows from being changed by users other than the Administrator, or by approved users authorized by the Administrator. (Based on MoReq 10.4.6)
- F10.1.9. The EDRMS should allow Administrators to designate that individual users are able to reassign tasks/actions to different users or user groups. (Based on MoReq 10.4.7)
- F10.1.10. The EDRMS should record all changes to programmed workflows in the audit trail. (Based on MoReq 10.4.8)
- F10.1.11. The EDRMS should record the progress of a record or file through a workflow so that users can determine the status of a record or file in the process. (Based on MoReq 10.4.9)
- F10.1.12. The EDRMS should not practically limit the number of workflows that can be defined. (Based on MoReq 10.4.10)
- F10.1.13. The EDRMS should support management of files and records in queues that can be examined or controlled by the Administrator and authorized users. (Based on MoReq 10.4.11)
- F10.1.14. The EDRMS should be capable of letting participants view queues of work addressed to them and select items to be worked on. (Based on MoReq 10.4.12)
- F10.1.15. The EDRMS should provide conditional flows depending on user input or system data. (Based on MoReq 10.4.13)
- F10.1.16. The EDRMS should provide a reminder, or bring-forward, facility for files and records. (Based on MoReq 10.4.14)
- F10.1.17. The EDRMS should allow users to pause or interrupt a flow (i.e., to suspend it) temporarily in order to be able to attend to other work. (Based on MoReq 10.4.15)
- F10.1.18. The EDRMS should recognize individuals and groups as participants in a workflow. (Based on MoReq 10.4.16)
- F10.1.19. The EDRMS should provide a facility to “load balance” by distributing incoming items to group members in rotation or based on a set of business rules defined by the Administrator. (Based on MoReq 10.4.17)
- F10.1.20. The EDRMS should provide an ability to prioritize items in queues. (Based on MoReq 10.4.18)
- F10.1.21. The EDRMS solution should be able to associate time limits with individual steps and/or process in each flow, and report items that are overdue according to these limits. (Based on MoReq 10.4.20)
- F10.1.22. The EDRMS should allow the receipt of electronic documents to trigger workflows automatically. (Based on MoReq 10.4.21)
- F10.1.23. The EDRMS should provide reporting facilities to allow management to monitor workflow volumes, performance and exceptions. (Based on MoReq 10.4.22)

- F10.1.24. The EDRMS workflow feature should prevent pre-programmed workflows from being changed by users other than the Administrator, or by approved users authorized by the Administrator. (Based on MoReq 10.4.6)

F10.2. Electronic Signatures

Note: It is assumed that a digital signature will need to be verified prior to entering the record, and the details of verification recorded once it has done so. It should not be necessary to routinely verify digitally signed records once they are registered, since they will be managed within the EDRMS in a manner that ensures authenticity.

- F10.2.1. The EDRMS should be able to retain the information relating to electronic signatures, encryption and details of related verification agencies. (Based on MoReq 10.5.1)
- F10.2.2. The EDRMS should have a structure, which permits the easy introduction of different electronic signature technologies. (Based on MoReq 10.5.2)
- F10.2.3. The EDRMS should be able to retain and preserve as metadata, details about the process of verification for an electronic signature, including:
- F10.2.3.1. the fact that the validity of the signature was checked;
 - F10.2.3.2. the Certification Authority with which the signature has been validated;
 - F10.2.3.3. the date and time that the checking occurred. (Based on MoReq 10.5.4)
- F10.2.4. The EDRMS should be capable of checking the validity of an electronic signature at the time of capture of the record. (Based on MoReq 10.5.5)
- F10.2.5. The EDRMS should include features which allow the integrity of records bearing electronic signatures to be maintained (and to prove it has been maintained), even though an Administrator has changed some of its metadata, but not the content of the record, after the electronic signature was applied to the record. (Based on MoReq 10.5.6)
- F10.2.6. The EDRMS should be able to store with the electronic record:
- F10.2.6.1. the electronic signature(s) associated with that record;
 - F10.2.6.2. the digital certificate(s) verifying the signature;
 - F10.2.6.3. any confirming counter-signatures appended by the certification authority in such a way that they are capable of being retrieved in conjunction with the record, and without prejudicing the integrity of a private key. (Based on MoReq 10.5.7)

F10.3. Encryption

- F10.3.1. Where an electronic record has been sent or received in encrypted form by a software application which interfaces with the EDRMS, the EDRMS should be capable of restricting access to that record to users listed as holding the relevant decryption key, in addition to any other access control allocated to that record. (Based on MoReq 10.6.1)
- F10.3.2. Where an electronic record has been transmitted in encrypted form by a software application which interfaces with the EDRMS, the EDRMS should be able to keep as metadata with that record:

F10.3.2.1. the fact of encrypted transmission;

F10.3.2.2. the type of algorithm;

F10.3.2.3. the level of encryption used. (Based on MoReq 10.6.2)

F10.3.3. The EDRMS should be able to ensure the capture of encrypted records directly from a software application which has an encrypting capability, and restrict access to those users listed as holding the relevant decryption key. (Based on MoReq 10.6.3)

F10.3.4. The EDRMS should allow encryption to be removed when a record is imported or captured. (Based on MoReq 10.6.4)

This feature may be desired in some large-scale record archives that have a requirement for long-term access (because encryption etc. is likely to reduce the ability to read records in the long term). In this case, the organisation would rely on audit trail or similar information to prove that the encryption etc. had been present but has been removed. In other environments, this feature may be undesirable from a legal point of view.

F10.3.5. The EDRMS should have a structure that permits different encryption technologies to be introduced easily. (Based on MoReq 10.6.5)

F10.4. Electronic Watermarks

F10.4.1. The EDRMS should be capable of storing records bearing electronic watermarks, and of storing with them information about the watermark. (Based on MoReq 10.7.1)

F10.4.2. The EDRMS should be able to retrieve information stored in electronic watermarks. (Based on MoReq 10.7.2)

F10.4.3. The EDRMS should have a structure that permits different watermarking technologies to be introduced easily. (Based on MoReq 10.7.3)

F11. General Requirements

F11.1. Ease of Use

F11.1.1. The EDRMS should enable users to access electronic document services from both client workstations and remotely connected computers; with:

F11.1.1.1. a full range of services delivered to desktop clients in a familiar windows environment;

F11.1.1.2. (at minimum) search, view and download services available to remote users.

F11.1.2. The EDRMS should fully support inter/intranet web based technology, where

- F11.1.2.1. web servers provide all necessary mechanisms to store and retrieve information requested by users, system level security for users and data, and system management functions;
- F11.1.2.2. web browsers provide a common user interface for accessing the EDRMS applications and document repositories.
- F11.1.3. The EDRMS should provide the ability of users to enable users to save information in user-selectable formats. At minimum, these should include:
 - F11.1.3.1. HTML;
 - F11.1.3.2. XML;
 - F11.1.3.3. PDF.
- F11.1.4. The EDRMS should support web publishing by providing:
 - F11.1.4.1. a mechanism for authorized users to create HTML and XML templates for specific classes or types of documents;
 - F11.1.4.2. convert documents to the above templates for web distribution.
- F11.1.5. The EDRMS should provide online help throughout the EDRMS. (Based on MoReq 11.1.1)
- F11.1.6. The online help in the EDRMS should be context-sensitive. (Based on MoReq 11.1.2)
- F11.1.7. All error messages produced by the EDRMS should be meaningful, so that they can be appropriately acted upon by the users who are likely to see them. (Based on MoReq 11.1.3)
- F11.1.8. The EDRMS should employ a single set of user interface rules, or a small number of sets. These should be consistent with the operating system environment in which the EDRMS operates. (Based on MoReq 11.1.4)
- F11.1.9. The EDRMS should be able to display several records simultaneously. (Based on MoReq 11.1.5).
- F11.1.10. Where the EDRMS uses on-screen windows, each should be user-configurable. (Based on MoReq 11.1.6)
- F11.1.11. The EDRMS user interface should be suitable for users with special needs; that is, compatible with specialist software that may be used and with appropriate interface guidelines (e.g., W3C Web Content Accessibility Guideline, Microsoft Official Guidelines for User Interface Developers and Designers). (Based on MoReq 11.1.7)
- F11.1.12. Where the EDRMS includes the use of windows, it should allow users to move, re-size and modify their appearance, and to save modifications in a user profile. (Based on MoReq 11.1.9)
- F11.1.13. The EDRMS should allow users to select sound and volume of audio alerts, and to save modifications in a user profile. (Based on MoReq 11.1.10)

- F11.1.14. The EDRMS should allow persistent defaults for data entry where desirable. These defaults should include:
- F11.1.14.1. user-definable values;
 - F11.1.14.2. values same as previous item;
 - F11.1.14.3. values derived from context, e.g., date, file reference, user identifier; as appropriate. (Based on MoReq 11.1.11)
- F11.1.15. The EDRMS should be closely integrated with MS Outlook in order to allow users to send electronic records and files electronically without leaving the EDRMS. (Based on MoReq 11.1.13)
- F11.1.16. The EDRMS should provide integration with MS Outlook by sending pointers to files and records rather than copies, whenever a file or record is sent to another user of the EDRMS. (Based on MoReq 11.1.14)
- F11.1.17. Where the EDRMS employs a graphical user interface, it should allow users to customize it. Customization should include, but need not be limited to the following changes:
- F11.1.17.1. menu contents;
 - F11.1.17.2. layout of screens;
 - F11.1.17.3. use of function keys;
 - F11.1.17.4. on-screen colours, fonts and font sizes;
 - F11.1.17.5. audible alerts. (Based on MoReq 11.1.15)
- F11.1.18. The EDRMS should support user-programmable functions. (Based on MoReq 11.1.16)
- For example, user-definable macros.*
- F11.1.19. The EDRMS should provide the capability to perform global data updates.
- F11.1.20. The EDRMS should allow users to define cross-references between related records, both within the same file and in different files, allowing easy navigation between the records. (Based on MoReq 11.1.17)
- F11.1.21. Where users have to enter metadata from images of printed documents, the EDRMS should provide features to allow the use of optical character recognition to capture metadata from the image (zoned optical character recognition). (Based on MoReq 11.1.17)
- F11.1.22. The EDRMS should allow users to define cross-references between related records, both within the same file and in different files, allowing easy navigation between the records. (Based on MoReq 11.1.18)

F11.2. Product Maturity and Currency

- F11.2.1. The EDRMS should use mature components, with each component having a history of regular updates to provide: new functionality, 'bug' fixes, adherence to new standards

and technologies, and continued integration with standard office applications and with current/emerging document-related applications. Such maturity and currency should be demonstrable/verifiable for the EDRMS:

- F11.2.1.1. document management component;
- F11.2.1.2. records management component for electronic records;
- F11.2.1.3. records management component for physical records. (Based on AIM, p. 20)

PROVIDE EVIDENCE OF THE ABILITY OF THE PROPOSED SOLUTION TO MEET THE PRODUCT MATURITY/CURRENCY REQUIREMENTS; E.G.:

- **IDENTIFY MAJOR NEW RELEASES/UPGRADES FOR EACH COMPONENT OVER THE PAST 2 YEARS**
- **IDENTIFY INTERFACES/INTEGRATION ACHIEVED OVER THE PAST 2 YEARS WITH RELATED APPLICATIONS/TECHNOLOGIES**

F11.3. Scalability

- F11.3.1. The EDRMS should be fully scaleable and should:
 - F11.3.1.1. NOT have any features that would preclude use in small or large organizations, with varying numbers of differently sized organizational units. (Based on MoReq 11.2.8)
 - F11.3.1.2. allow for an increase of the number of users and volumes of data without replacing primary system components (i.e., scalability in terms of increased memory, disk storage, optical storage, CPU speed and size, etc.). (AIIM p. 19)
 - F11.3.1.3. NOT impose limits the on numbers of classification elements, files/volumes, or records. (Based on MoReq 3.2.9)
 - F11.3.1.4. The EDRMS applications should have a high degree of modularity, allowing for implementation of additional functionality without adversely affecting the overall system (i.e., ability to add routing, OCR, automated fax services, workload distribution, form management, etc.). (AIIM, p. 9)
- F11.3.2. The EDRMS should meet the following criteria for enterprise-wide implementation within the context of the BC government:

- F11.3.2.1. ability to deploy EDRMS application(s) to every employee desktop ;
- F11.3.2.2. support for large numbers of users who could require access to a single document repository or to multiple repositories;
- F11.3.2.3. support for a distributed environment where multiple repositories (databases, servers, optical jukeboxes, etc.) exist in multiple, widely dispersed geographic locations;
- F11.3.2.4. support replication between repositories;
- F11.3.2.5. integrate with a wide range of technologies to be found within the crown corporations and ministries of the BC government;
- F11.3.2.6. provide tools for monitoring and tuning system performance.
- F11.3.3. All components of the EDRMS solution should be equally scalable and robust.

ATTACH A DESCRIPTION OF THE ABILITY OF THE PROPOSED SOLUTION TO MEET THE SCALABILITY REQUIREMENTS; E.G.,

- **DESCRIPTIONS OF THE LARGEST INSTALLATION/TESTING DONE TO DATE, INCLUDING NUMBER AND TYPES OF SERVERS, NUMBER OF TOTAL USERS, NUMBER OF AVERAGE CONCURRENT USERS, NUMBER OF RECORDS STORED, DATA SIZE OF RECORDS STORED (IN TERABYTES), INDEX/METADATA SIZE (IN GIGA/TERABYTES), SEARCH RESPONSE TIME, FILE ACCESS TIME, ETC.**

F11.4. Performance

- F11.4.1. The EDRMS should provide adequate response times for commonly performed functions under standard conditions;
 - F11.4.1.1. 75% of the total user population for a particular repository/organization logged on and active (potentially several thousand concurrent users);
 - F11.4.1.2. users performing a mix of system functions at various rates. (Based on MoReq 11.2.1)
- F11.4.2. The EDRMS should be able to perform a simple search within 3 seconds and a complex search (combining four terms) within 10 seconds regardless of the storage capacity or number of files and records on the system. (Based on MoReq 11.2.2)

In this context, performing a search means returning a result list. It does not include retrieving the records themselves.

- F11.4.3. The EDRMS should be able to retrieve and display within 4 seconds the first page of a record that has been accessed within the previous 3 months, regardless of storage capacity or number of files/records on the system. (Based on MoReq 11.2.3)

This requirement is intended to allow for rapid retrieval of frequently used records, on the understanding that frequency of use is typically correlated with recent use.

- F11.4.4. The EDRMS should be able to retrieve and display within 20 seconds the first page of a record that has not been accessed within the previous 3 months, regardless of storage capacity or number of files/records on the system. . (Based on MoReq 11.2.4)

This requirement is intended to allow for cases where a form of hierarchical storage management is used, where records used infrequently are stored on slower media than more active records.

- F11.4.5. It should be possible to expand the EDRMS, in a controlled manner, up to at least 30 thousand users while providing effective continuity of service. (Based on MoReq 11.2.6)

- F11.4.6. The EDRMS should support the above scalability requirements, including routine maintenance of:

- F11.4.6.1. user and group data;
- F11.4.6.2. access profiles;
- F11.4.6.3. classification schemes;
- F11.4.6.4. databases;
- F11.4.6.5. retention schedules;

in the face of the anticipated levels of organisational change, without imposing undue systems/account administration overheads. (Based on MoReq 11.2.7)

F11.5. Openness, Connectivity and Standards

- F11.5.1. The EDRMS should utilize industry standard components (without proprietary architectures), commonly available throughout the document management, imaging and workflow industries. (Based on AIIM, p. 13)
- F11.5.2. The EDRMS should use industry standard interfaces for any scanning interface proposed, e.g. TWIN and ISIS.
- F11.5.3. The proponent should indicate which third party document scanning/conversion applications they support or have successfully integrated with.
- F11.5.4. The proponent should indicate what/which storage systems are supported e.g. drives and raw access; via the file system and data files; or file system and native record objects.
- F11.5.5. The document management portion of the EDRMS should meet recommended industry standards, including:

- F11.5.5.1. adherence to the Association for Information and Image Management's (AIIM) Document Management Alliance Specification (DMA) for software component interoperability;
- F11.5.5.2. adherence to the Open Document Management API (ODMA) specifications for application programming interfaces. (Based on AIIM, pp. 13, 19, 28)
- F11.5.6. The document management portion of the EDRMS should provide a rich set of programming interfaces that will integrate with applications as the BC government brings them into use. The EDRMS should enable the users to write applications, either client-server or thin client that will operate on MS Windows desktops, in one or more languages such as:
- F11.5.6.1. Java;
- F11.5.6.2. Visual Basic;
- F11.5.6.3. C++
- F11.5.6.4. Proprietary scripting/development environment.
- F11.5.7. The document management portion of the EDRMS should support or provide the ability to build web-based access to documents in the system. This requirement means that the proposed solution should be able to transfer/receive information, metadata and records to/from an Enterprise Portal application for inter/intranet access.

THE PROPONENT SHOULD INDICATE WHICH PORTAL SOFTWARE THE PROPOSED DOCUMENT MANAGEMENT SYSTEM HAS BEEN LINKED TO.

- F11.5.8. The EDRMS should support the storage of records using file formats and encoding which are either de jure standards or which are fully documented. (Based on MoReq 11.4.4)
- F11.5.9. The EDRMS should conform to the search and retrieval and information exchange standards, including ISO 23950, Information retrieval – application service definition and protocol specification (ANSI Z39.50). (Based on MoReq 11.4.5)
- F11.5.10. Relational databases used by the EDRMS should conform to the SQL standard, ISO/IEC 9075, Information technology – database languages – SQL (Based on MoReq 11.4.6)
- F11.5.11. The EDRMS should store all country names in a format compliant with ISO 3166, Codes for the representation of names of countries. (Based on MoReq 11.4.8)
- F11.5.12. The EDRMS should store all language names in a format compliant with ISO 639, Codes for the representation of names of languages. (Based on MoReq 11.4.9)
- F11.5.13. If the EDRMS is to manage records in multiple languages or using non-English characters, it should be capable of handling ISO 8859-1 encoding. (Based on MoReq 11.4.10)
- F11.5.14. If the EDRMS is to manage records in multiple languages or using non-English characters, it should be capable of handling ISO 10646 encoding (Unicode). (Based on MoReq 11.4.11)

F12. Technical Requirements

F12.1. Ability to Operate within BC Government Technology Infrastructure

- F12.1.1. The EDRMS should be capable of operating within the current BC government Technology Infrastructure as outlined in **Appendix I** of this RFP.

ATTACH AN EXPLANATION OF THE PROPOSED APPROACH FOR MEETING THE TECHNICAL REQUIREMENTS; E.G.:

- **ABILITY OF THE PROPOSED EDRMS APPLICATION TO MEET THE REQUIREMENT “OUT OF THE BOX”;**
- **REQUIRED APPLICATION CUSTOMIZATION;**
- **OTHER RELEVANT CONSIDERATIONS, INCLUDING ANY PRACTICAL LIMITS ON THE SIZE OF THE ELETRONIC RECORD STORE (X TERABYTES/X MILLION RECORDS) AND NUMBER OF USERS ABLE TO CONCURRENTLY USE THE EDRMS OR A PARTICULAR REPOSITORY WITHIN THE EDRMS.**

Appendix G Draft Meta-Data Elements

G1 Introduction

This appendix provides a preliminary overview of the types of metadata required in a BC government EDRM system, along with notes on anticipated metadata characteristics and sources.

Categories of metadata include:

- **Classification and scheduling** metadata -- e.g., attributes of schedule, primary and secondary records maintained within the ARCS/ORCS master database (See **Appendix H**).
- **File and Volume metadata** -- i.e., attributes of file and volume records maintained in the EDRMS.
- **Offsite transfer metadata** -- i.e., attributes of the accession, service application and container records maintained in the EDRMS to document the transfer of batches of containers (housing records) to offsite storage facilities and/or archival custody.

Note: The metadata listed for the above types of database records are those elements that the EDRMS will need to associate with the records profiles below (e.g., by having the elements “cascade down” into the profiles and by linking the records profiles to the classification/scheduling, file/volume and offsite transfer records.)

- **Records Profile metadata** -- i.e., the descriptive elements used to identify particular records managed by the EDRMS. The EDRMS must be capable of maintaining profiles for electronic records stored within in the EDRMS repositories and for physical records stored outside of the EDRMS.

Note: It is assumed that only a basic subset of the listed elements will be designated as mandatory, and that some of the elements are specific to particular types of records (e.g., e-mail). Also, if the document management application within the EDRMS were used to manage documents that are not captured/managed as records, only a small subset of the records profile metadata would be required for these documents.

G2. Classification and Scheduling metadata elements

Ref.	Metadata element	Type/Size	Information Source/Notes
G.2.1	Schedule number	Numeric: 6 (e.g., 100001)	ARCS/ORCS database (see Appendix H)
G.2.2	Schedule amendment number	Numeric: 6 (e.g., 105500)	ARCS/ORCS database (see Appendix H)
G.2.3	Schedule status (approved/draft)	Logical [Y/N] or alphabetic (e.g., A, D)	ARCS/ORCS database (see Appendix H)
G.2.4	Schedule title	Alphanumeric	ARCS/ORCS database (see Appendix H)
G.2.5	Primary number	Numeric: 3, 4, or 5 (e.g., 100; 6450, 13500)	ARCS/ORCS database (see Appendix H)
G.2.6	Primary title	Alphanumeric	ARCS/ORCS database (see Appendix H)
G.2.7	Secondary number	Numeric: 2 digits	ARCS/ORCS database (see Appendix H)
G.2.8	Secondary title	Alphanumeric	ARCS/ORCS database (see Appendix H)
G.2.9	OPR active retention code/time	Alphanumeric (e.g., code: CY; time: 1Y)	ARCS/ORCS database (see Appendix H)
G.2.10	NonOPR active retention code/time	Alphanumeric (e.g., code: FY; time: 2Y)	ARCS/ORCS database (see Appendix H)
G.2.11	OPR semi-active /near line retention code/time	Alphanumeric (e.g., code: Nil; time: 5Y)	ARCS/ORCS database (see Appendix H)
G.2.12	Non-OPR semi-active/near line retention code/time	Alphanumeric (e.g., code: NA; time: 2Y)	ARCS/ORCS database (see Appendix H)
G2.13	Security classification (e.g., Protected Cabinet, Protected)	Alphanumeric	ARCS/ORCS database, secondary flag (see Appendix H)
G2.14	FOI access status codes (e.g., FOI Review Required, Routine Disclosure, Outside Scope of Act)	Alphanumeric	ARCS/ORCS database, secondary flag (see Appendix H)
G2.15	Privacy designation/personal information codes (e.g., PIB, Sensitive Personal, Public Personal, Non-personal)	Alphanumeric	ARCS/ORCS database, secondary flag (see Appendix H)
G.2.16	Vital records indicator	Alphanumeric	ARCS/ORCS database, secondary flag (see Appendix H)
G.2.17	User-defined elements		

G3. File and Volume metadata elements

Ref.	Metadata element	Type/Size	Information Source/Notes
G3.1	Unique identifier - file	Numeric	
G3.2	File code	Alphanumeric	
G3.4	File title	Alphanumeric	
G3.5	File opened date	Date	
G3.6	File closed date	Date	Date when file is generally closed to addition of new records (subject to authorised exceptions)
G3.7	File schedule trigger date (“cut-off” date)	Date	May differ from file close date
G3.8	File first record date	Date	Cascade up from earliest volume first record date
G3.9	File last record date	Date	Cascade up from latest volume last record date
G3.10	File description	Alphanumeric	
G3.11	Unique identifier - volume		Generated by EDRMS
G3.12	Volume identifier	Alphanumeric	[e.g., Volume 1]
G3.13	Volume description	Alphanumeric	
G3.14	OPR (office of primary responsibility)	Logical [Y/N]	
G3.15	Permanent location - electronic volume	Alphanumeric	Maintained by EDRMS
G3.16	Hybrid records indicator - volume	Logical [Y/N]	
G3.17	Organisation code and name (associated with one or more organisation roles)	Code: numeric, 5; name: alphanumeric	Ideally code and name are selected from ARIS Name Authority table (See Appendix H.4.3); automatically captured where possible
G3.18	Organisation role (e.g., OPR, Current Legal Custodian; Creator)	Alphanumeric	
G3.19	Security classification (e.g., Protected Cabinet, Protected)	Alphanumeric	Could cascade from schedule/classification metadata, with user override option
G3.20	Access rights [C,R,U,D]		EDRMS security matrix; group and user rights
G3.21	Volume first record date	Date	
G3.22	Volume last record date	Date	
G3.23	No further records added flag	Logical [Y/N]	
G3.24	Hold (suspend) actions	Logical [Y/N]	May require multiple hold flags for different actions (e.g., a hold on disposition action)

G3.25	Disposition action code	Alphanumeric	E.g., destruction/deletion; transfer to archives for selective retention
G3.26	Eligible disposition date	Date	Calculated by EDRMS from secondary retention times and file to/from dates
G3.27	Actual disposition date	Date	
G3.28	Disposition authorisation		
G3.29	Destruction confirmation status	Logical [Y/N]	
G3.30	Media designation code		
G3.31	Location		Applies to physical volumes
G3.32	Check-out/check-in status		Applies to physical volumes
G3.33	Date checked out		Applies to physical volumes
G3.34	Checked out to [person/unit]		Applies to physical volumes
G3.35	Bring forward date		Applies to physical volumes
G3.36	Bring forward to [person/unit]		Applies to physical volumes
G3.37	Bring forward comment		Applies to physical volumes
G3.38	FOI access status codes (e.g., FOI review required, Routine Disclosure, Outside scope of Act)	Alphanumeric	Could cascade from classification/scheduling metadata, with user override option
G3.39	Privacy Designation/Personal Information codes (e.g., PIB, sensitive personal, public personal, non-personal)	Alphanumeric	Could cascade from classification/scheduling metadata, with user override option
G3.40	Vital records indicator	Logical [Y/N]	Could cascade from classification/scheduling metadata, with user override option
G3.41	User-defined elements		

G4. Offsite transfer metadata elements

Note: The EDRMS may maintain these in accession/batch records, container records, etc. Volumes transferred to offsite facilities will need to be linked to the numbers of the accession/containers in which they are transferred.

Ref.	Metadata element	Type/Size	Information Source/Notes
G4.1	Accession number	Numeric: 6 (e.g., 921234)	ARIS
G4.2	Access authorisation (names of persons authorised to access/retrieve containers from offsite storage)		Currently maintained in ARIS; could be coordinated with EDRMS Security Matrix
G4.3	Application number (service application to transfer records offsite)	Numeric: 6 (e.g., 110456)	BC Archives forms (e.g., ARS517 form)
G4.4	Organisation code and name (associated with one or more organisation roles)	Code: numeric, 8; name: alphanumeric	Ideally code and name are selected from ARIS Name Authority table (See Appendix H.4.3)
G4.5	Organisation role (e.g., Transferring Agent)	Alphanumeric	
G4.6	Range of containers (covered by a particular application)	Numeric: 14 (e.g., 921234-0001-9999)	ARIS container numbers are comprised of: a 6 digit container ID (e.g., 921234) and a box number range (e.g., 0001)
G4.7	Container number	Numeric: 10 (e.g., 921234-0001)	ARIS container numbers are comprised of: a 6 digit container ID (e.g., 921234) and a box number range (e.g., 0001)
G4.8	Container format/size	Alphanumeric	
G4.9	Container location	Alphanumeric	May be expressed as multiple elements (storage facility, type of storage (e.g., archival, vital records, etc.))
G4.10	Container disposition dates (rolled up from files within the containers: e.g., eligible disposition date, actual disposition date)		Generated by EDRMS from file/volume data
G4.11	Contact information		Name, address, tel. no., etc. of person submitting/responsible for the service application
G4.12	User specified elements		

G5 Records profile metadata elements

Ref.	Metadata element	Type/Size	Information Source/Notes
G5.1	Unique identifier	Numeric	Generated by EDRMS
G5.2	Record name/title	Alphanumeric	
G5.3	Creator/Author	Numeric or alphabetic	Automatically captured from operating system, where possible
G5.4	Organisation code and name (associated with one or more organisation roles)	Code: numeric, 8; name: alphanumeric	Cascade from file/volume, with user override option
G5.5	Organisation role (e.g., records creator)	Alphanumeric	Cascade from file/volume, with user override option
G5.6	Person/position responsible for maintaining/posting record to EDRMS	Alphanumeric	Automatically captured from operating system, where possible
G5.7	Subject	Alphanumeric	Automatically captured from re. line in emails
G5.8	Creation date	Date	Automatically captured where possible
G5.9	Registration date	Date	Automatically captured from re. line in emails
G5.10	Compilation date	Date	E.g., start and end times of an audio recording; automatically captured where possible
G5.11	Date sent	Date	E.g., for e-mail; automatically captured where possible
G5.12	Date received	Date	E.g., for e-mail; automatically captured where possible
G5.13	Addressee	Alphanumeric	E.g., for e-mail; automatically captured where possible
G5.14	Sender [from]	Alphanumeric	E.g., for e-mail; automatically captured where possible
G5.15	Other recipients [to]	Alphanumeric	E.g., for e-mail; automatically captured where possible
G5.16	Hardware dependencies		Could be expressed as multiple elements
G5.17	Operating system dependencies		Could be expressed as multiple elements
G5.18	Application software dependencies		Could be expressed as multiple elements
G5.19	Record type		E.g., letter, memo etc.; automatically captured where possible
G5.20	Record format		Could be expressed as multiple elements
G5.21	Resolution		Could be expressed as multiple elements
G5.22	Compression algorithm version and parameters		Could be expressed as multiple elements
G5.23	Encoding scheme		Could be expressed as multiple elements

G5.24	Rendition information		Could be expressed as multiple elements
G5.25	Electronic signatures/certificate	Flag [Y/N]	
G5.26	Electronic signature authentication	Flag [Y/N]	Includes date and time checked
G5.27	Electronic watermark information		
G5.28	Encryption information		
G5.29	Links to related records		
G5.30	Email attachments	Logic field [Y/N]	
G5.31	Language		
G5.32	Preservation/migration history (e.g., action type, action date, description, migration schedule)		E.g., conversion/migration such as Word Perfect converted to MS Word 2000; paper to microform; electronic record to COLD; could be expressed as multiple elements
G5.33	Use history /management history (e.g., event dates, event type)		Could be expressed as multiple elements; may be maintained in audit log rather than in records profile
G5.34	Version	Numeric	
G5.35	Security classification (e.g., Protected Cabinet, Protected)	Alphanumeric	Could cascade from file/volume metadata, with user override option
G5.36	Access rights [C,R,U,D]		EDRMS security matrix; group and user rights
G5.37	FOI access status codes (e.g., FOI Review Required, Routine Disclosure, Outside Scope of Act)	Alphanumeric	Could cascade from file/volume metadata, with user override option
G5.38	Privacy Designation/Personal Information codes (e.g., PIB, Sensitive Personal, Public Personal, Non-personal)	Alphanumeric	Could cascade from file/volume metadata, with user override option
G5.39	Vital records indicator	Logical [Y/N]	Could cascade from file/volume metadata, with user override option
G5.40	Copyright/intellectual property rights		
G5.41	User-defined metadata		

Appendix H ARCS/ORCS Master Database

H1. Background

BC Archives has defined preliminary systems design requirements for an *ARCS/ORCS* Master Database Development Project. This project is intended to provide an electronic capability to support government-wide *ARCS/ORCS* development, maintenance and approval processes.

Details regarding this project are outlined below in order to provide respondents to the EDRMS RFP with information regarding the nature of the envisaged *ARCS/ORCS* application, which (if constructed) is intended to be interfaced/integrated with EDRMS to provide the EDRMS with records classification, retention and disposition data.

H2. Project Overview

This project includes replacing the current paper-based *ARCS/ORCS* with an Oracle database application, including various Web based access and update components. In addition to providing access, review and approval processes, the *ARCS/ORCS* application will support the transfer of required data between BC Archives and the various external organisations that are subject to the government's Public Documents legislation.

The project envisages:

- Development of a central Oracle database repository for managing draft and master (approved/published) copies of the BC government Administrative Records Classification System (*ARCS*), Operational Records Classifications Systems (*ORCS*) and other continuing schedules.
- Provision of a front-end application for creating, updating and deleting records in the *ARCS/ORCS* database.
- Provision of a web based application that replicates the current functionality of ARCS-Online (<http://www.bcarchives.gov.bc.ca/arcs/index.htm>) and that also provides web access to ORCS and other schedules maintained in the central repository.
- Provision of a utility to track updates to information in the database for historical tracking purposes. (At key points in time, a Schedule as it existed at that point must be able to be recreated for online display and printing purposes.)
- Develop any required printing/data export (e.g. XML) capability for *ORCS* review and archival preservation of *ARCS/ORCS* publications.
- Develop required remote data entry capabilities (web forms/e-forms).
- Provision of intelligent records management e-forms – to provide automated data entry and verification functions for records management e-forms such as BC Archives service application forms.
- Provision of automated updates to ministry EDRMS and RM applications by providing a common source of data for loading *ARCS/ORCS*.

H3 Central ARCS/ORCS Oracle Database

The central Oracle database repository is expected to include the entities listed below. Entities that will contain schedule and classification data intended for export to the EDRMS are displayed in bold, along with a selected list of key data elements.

Note: This assumes that the ARCS/ORCS Database is used for schedule/classification development, approval and publication processes. If these functions were performed within the EDRMS, it may also require non-bolded items.

H3.1 Records Schedules

- **Data drawn from ARIS (see section H.4)**

H3.2 Schedule Tracking Records

- **Data drawn from ARIS (see section H.4)**

H3.3 Executive Summary (for Schedule and Schedule Amendments)

H3.4 Agencies Responsible (Organisational Name Authorities)

H3.5 **OPR Generic** (Generic terms for types of Offices of Primary Responsibility)

- **Obsolete_Date; OPR_ID; OPR_Name**

H3.6 **OPR offices** (Organisational Names of Office of Primary Responsibility)

- **Data drawn from ARIS Name Authorities (see section H.4)**

H3.7 Sections

- **Primary_End, Primary_Start, Schedule_Auth_ID, Section_Description, Section_Name, Status_ID**

H3.8 Primary Blocks

- **Block_ID; Parent_ID; Primary_Block_Title; Schedule_Auth_ID**

H3.9 Primaries

- **NonOPR_Active_Retention_Code; NonOPR_Active_Retention_Time; NonOPR_Final_Disposition_Code; NonOPR_Semiactive_Retention_Code; NonOPR_Semiactive_Retention_Time; OPR_Active_Retention_Code; OPR_Active_Retention_Time; OPR_Final_Disposition_Code; OPR_Generic_ID; OPR_Name_Authority_ID; OPR_Semiactive-Retention_Code; OPR_Semiactive_Retention_Time; Primary_ID; Primary_Number; Primary_Title; Schedule_Auth_ID; Scope_Note; Superseded_by**

H3.10 Primary Cross References

- **Primary_ID; Text_Before; Xref_ID; Xref_Number; Xref_Type**

H3.11 Secondaries

- **NonOPR_Active_Retention_Code; NonOPR_Active_Retention_Time; NonOPR_Final_Disposition_Code; NonOPR_Semiactive_Retention_Code; NonOPR_Semiactive_Retention_Time; OPR_Active_Retention_Code; OPR_Active_Retention_Time; OPR_Final_Disposition_Code;**

OPR_Generic_ID; OPR_Name_Authority_ID; OPR_Semiactive-Retention_Code; OPR_Semiactive_Retention_Time; Primary_ID; Secondary_ID; Secondary_Number; Secondary_Title; Use_Primary_Default_NonOPR_Retention; Use_Primary_Default_OPR_Retention

H3.12 Secondary Flags such as PIB (Personal Information Bank), PUR (Public Use Record), VR (Vital Records)

- **Description, Flag_Code, Flag_ID**

H3.13 Notes for Primaries and Secondaries

- **Applies_To; Note_Code; Note_ID; Note_Text; Note_Type_ID; Order_Indicator; Primary_ID; Secondary_ID; Status_ID**

H3.14 ISOs (Information System Overview)

H3.15 Lists of Primaries/Secondaries which describe ISO processes

- ISO Cross References

H3.16 Description of how to use the Subject Index

H3.17 Subject Index

D.3.18 Appendices

H4 ARIS Schedule and Name Authority Data

The Schedule, Schedule Amendment and Name Authorities information required by the ARCS/ORCS database is maintained in the BC Archives Oracle-based ARIS (Archives and Records Information System) application. The ARCS/ORCS system will incorporate replicate copies of the following ARIS tables:

H4.1 Schedule Authority Table

- **Final_Disposition_Hold_Flag; From_Date; ID; Number; Schedule_Auth_Type; To_Date; Type_CD**

H4.2 Schedule Tracking Table

- **Amendment_Num; Approval_DT; ID; Notes; Schedule_ID_Tracked; Schedule_Auth_Num; Schedule_Auth_Type; Schedule_Tracking_Type; Status_CD; Title; Type_CD**

H4.3 Name Authority Table

- **End_Date; ID; Lvl_1_Name_Desc; Lvl_2_Name_Desc; Lvl_3_Name_Desc; Lvl_4_Name_Desc; Lvl_5_Name_Desc; Lvl_6_Name_Desc; Lvl_7_Name_Desc; Lvl_8_Name_Desc; ; Lvl_1_Name_ID_Parent; Lvl_2_Name_ID_Parent; Lvl_3_Name_ID_Parent; Lvl_4_Name_ID_Parent; Lvl_5_Name_ID_Parent; Lvl_6_Name_ID_Parent; Lvl_7_Name_ID_Parent; Lvl_8_Name_ID_Parent; Lvl_CD; Name_Desc; Name_ID_Parent; Start_Date**

Below is a partial screen print of an ARIS Name Authority record:

Archives and Records Information System

Action Edit Field Record Query ServReq Acgn Appl MU Cntr Sched/Acq Peop/Addr NA Navigation Reports Admin Window Help

Normal Mode

Maintain Existing Name Authorities

Lowest Level Name: British Columbia Archives

ID: 33793

Name Authority Level: 4

Name Use Start Date: 1998-07-20

Name Use End Date: 2001-06-04

Level 1 Name	British Columbia	1858-08-02	
Level 2 Name	Information, Science and Technology Agency	1997-04-01	2001-06-04
Level 3 Name	Information Management and Corporate Policy Division	1998-07-20	2001-06-04
Level 4 Name	British Columbia Archives		
Level 5 Name			
Level 6 Name			
Level 7 Name			
Level 8 Name			

Type of Name: C

Name Use Start Date Note: [Empty]

Name Use End Date Note: [Empty]

Verification Level: 2

RAD Form of Name: [Empty]

Verification Date: 1998-12-14

Lowest level name in the Name Authority hierarchy
Count: 1

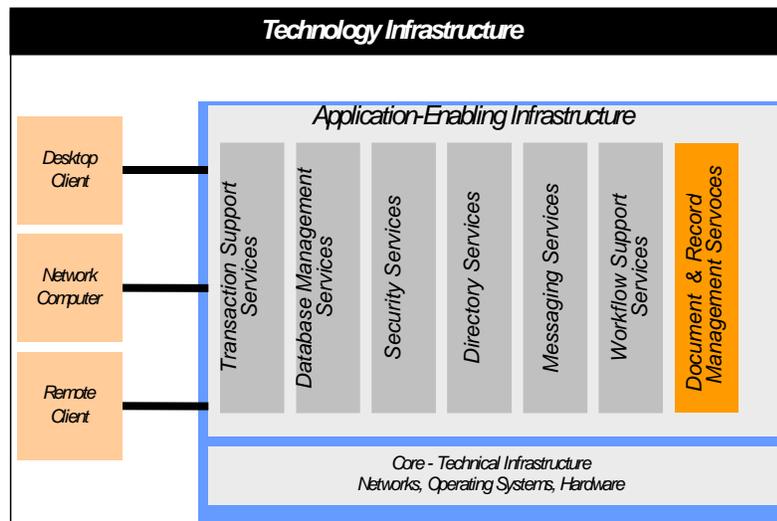
Appendix I Technology Infrastructure

1. The Province's Architecture Framework

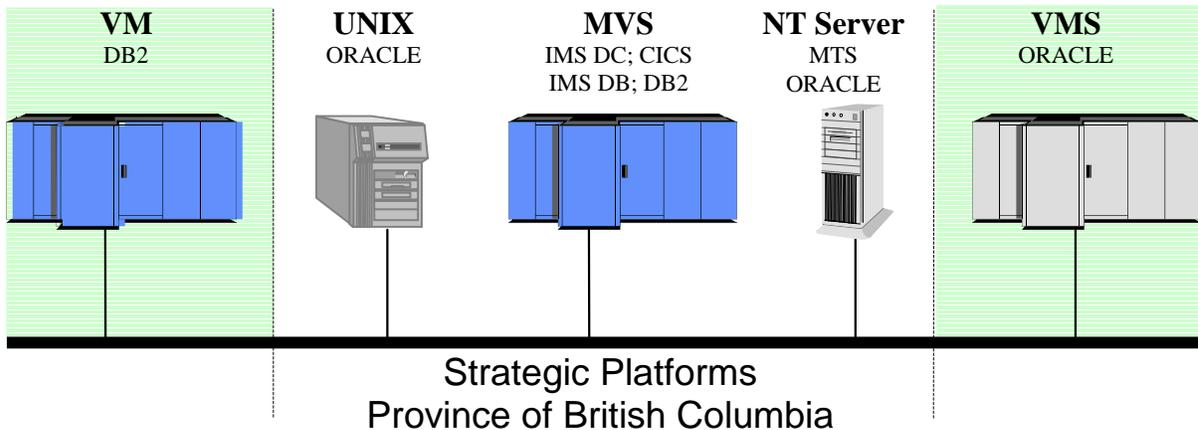
The following outlines the Province of British Columbia Technology Infrastructure as it relates to the EDRMS. The EDRMS will be managed by the government's Information, Technology and Services Division (ITSD) as a shared service.

The proponent should indicate his preferred server technology and indicate his percent of installations for that selected technology and other technologies.

The following is a conceptual diagram of the government's technology infrastructure.



Over time, government Line of Business applications have been implemented on a wide variety of application platforms as shown below. Government has defined IBM OS/390, Microsoft Windows NT/2000/XP and UNIX as the strategic platforms to be used for new application deployment. In the future there may be a requirement to obtain metadata contained in any of the following LOB Application Platforms:



Much of the material in this Appendix is taken from a recent RFP for an Integration Broker and is provided as background. A VM, MVS or VMS solution will not be acceptable

2. Unix Environment

The UNIX environment consists of 300-500 servers from multiple vendors, with the largest installed bases being from Sun, IBM and Compaq/Digital. Data General, NCR, and HP servers are also being used. Most of the servers accessing and running database environments do so using Oracle, although Informix and Sybase are in use at some sites. In addition to the many sites running Apache and Oracle web servers are some specialized applications, of which the manipulation of spatial data is but one example.

The servers are geographically dispersed throughout the province, with the largest concentrations being located in the Vancouver and Victoria metropolitan areas. Some computing environments in Victoria are being replicated to Vancouver for the purpose of Disaster Recovery. The Unix servers currently access about 25 terabytes of disk storage, which is forecasted to increase to over 45 terabytes in the next 12 months.

The UNIX environment is also host to a state-of-the-art hardware and software environment for network backup and restore of local server data and a limited number of its' network attached remote servers. That environment is using Veritas DataCentre NetBackup with two media servers, one onsite (a Sun E450 attached to a Sun L700 tape robot) and the other offsite (a Digital Alpha 2100 4/275 attached to a Digital TL893 robot) each holding about 300 tapes.

3. Microsoft Environment

Government's Microsoft Windows environment consists of a desktop and server infrastructure supporting approximately 35,000 desktops and several hundred servers. The desktops are a combination of Windows NT4, Windows 2000, Windows XP Pro, UNIX and thin client terminal devices. The UNIX and thin client devices access Windows terminal services operating Citrix Metaframe servers or Windows Terminal Services. Current plans target the retirement of NT 4 by March 2003, with all desktops upgraded to a combination of Windows 2000/Windows XP Pro or thin client devices (with access to Windows 2000 WTS or Metaframe servers). The Windows server infrastructure includes messaging services (i.e. MS Exchange), NT File and Print Services, Web hosting using IIS, custom applications written in a variety of development languages, Oracle database servers and active directory servers.

3.1 Authentication and Directory Infrastructure

3.1.1 NT4 Shared Infrastructure

The BC government's NT 4.0 shared domain infrastructure is characterized a government-wide multi-master domain model, consisting of three (3) master domains (BCGOV1, BCGOV2 and BCGOV3). Each of these three domains support account and machine credentials for Victoria, Vancouver and the rest of the province respectively. Separate resource domains support the various application categories (e.g. Exchange, File, Print, and Custom Applications).

3.1.2 NT4 Dedicated Infrastructure

In addition to the NT4 Shared Infrastructure a variety of NT4 domains exist for multiple ministries and agencies that do not fully utilize the NT4 Shared Infrastructure.

3.1.3 Windows 2000 Shared Infrastructure

The government is currently in the process of migrating its NT4 Shared Infrastructure and NT4 Dedicated Infrastructures into a single Windows 2000 Shared Infrastructure. Concurrent operation of these three infrastructures is expected to continue until the completion of the government's Windows 2000 migration (March 2003).

The Window 2000 tree and forest design is characterized by a single forest with a single tree structure which consists of a shell "root" domain (BCGOV) with an internal "**Core Government**" domain (IDIR.BCGOV) and an external "**Business Partners**" domain (BceID).

The '**Core Government**' domain (IDIR.BCGOV) consists of the approximate 40,000 staff members of government Ministries and Agencies. Initially, this domain's OU design will have one OU per ministry or agency. This domain provides:

- Delegated administration;
- Flexible OU structure;
- Access to line of business applications;

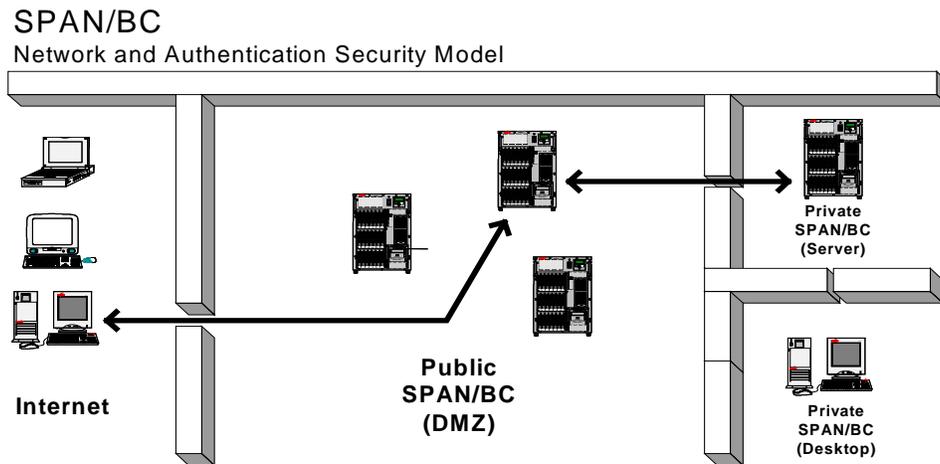
Shared government Email;
Desktop & LAN services;
Authentication and Authorization;
PKI security.

Note: Access to this domain will be either by internal Span/BC, or external VPN only.

The “**Business Partners**” domain (BCEID) consists of ‘Government Business Partners’ and other ‘Sponsored’ users of government line of business applications. These business partners are organizations requiring authenticated access to government line of business applications. Initially this domain’s OU design will have one OU per participating organization.

3.2 Network Topology – Private, Public, and DMZ zones.

The network topology supporting Windows 2000 will divide the SPAN/BC TCP/IP network into four distinct security zones: Internet, Shared Private Network or DMZ, Private Server and Private Desktop. All Windows 2000 active directory, DNS, and WINS services fall within the Private Server zone.

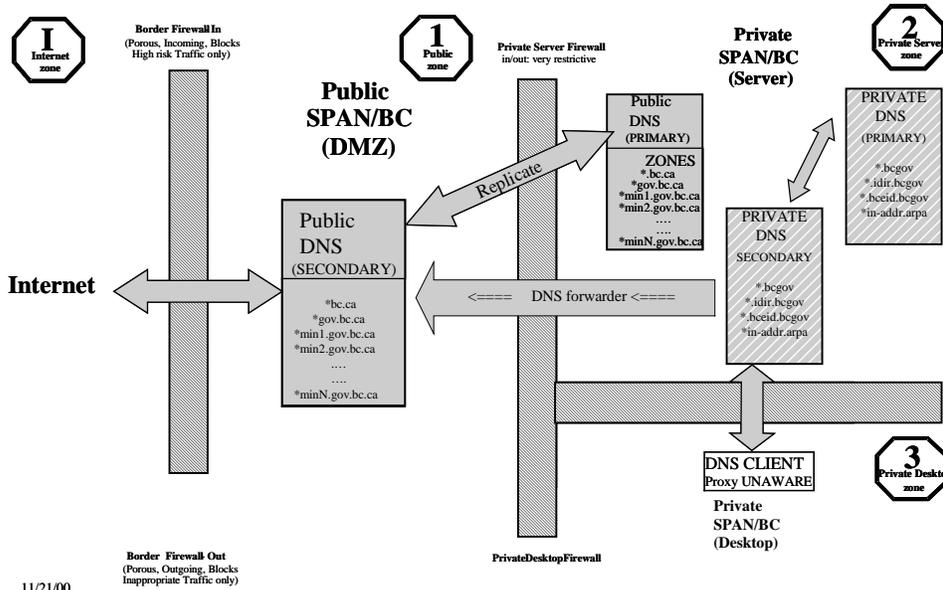


The firewall mechanism between the zones is implemented using router ACL’s in the SPAN/BC network and only allows appropriate TCP/IP connections.

3.3 DNS Considerations

The government DNS service architecture includes both external (public) and internal (private) zones. The external zones allow Internet and DMZ clients to resolve names of government services that are for public use. The internal (private) zones are only available to clients from the private server and desktop network zones. The following diagram shows the public/private split of the DNS service.

Network SPLIT DNS Security Model



3.4 Active Directory and DNS Zones

Each Windows 2000 domain constitutes its own DNS zone. Only Windows 2000 workstations, member servers and domain controllers will be in the Windows 2000 DNS zones (idir.bcgov and BCEID).

The root domain BCGOV zone and any other internal DNS zones can contain hostnames for Unix, VMS, and other systems not supporting secure dynamic updates to the Windows 2000 DNS server. These hosts will be registered statically within the root domain servers.

4. Desktop, Local Area Network and Office System Environment

The government has approximately 34,000 desktop computers, most running government's standard Microsoft Windows NT desktop operating system, although a number still run Windows 95 or Windows 98. Approximately 80% of these government desktop computers are located in Greater Victoria and in Greater Vancouver. The remainder is located in District and Regional facilities throughout the province. Government's corporate standard for office productivity software is Microsoft Office.

Operating system and office productivity software releases are managed centrally across government.

With the introduction of Windows XP and Office XP over the course of the next few years it is planned that government will migrate its desktops and office systems as follows:

Asset	Current Standard	Future Direction
Desktop	Windows NT Windows 2000	Windows 2000, Windows XP
Office	Office 2000	Office XP

Local Area and Wide Area Network Environments

Typically, desktops are attached to local area networks (LAN) implemented using government's standard Microsoft Windows NT LAN operating system, although a few residual LANs based on other technologies remain to be converted. These LANs are primarily connected to government's corporate wide area SPAN/BC network using TCP/IP. Most rural locations average 56KB connections to the WAN, while locations in the more urban areas usually are supported with higher bandwidth connections.

The corporate Office Information System (OIS) for government including electronic mail, calendar and directory functionality is based on Microsoft Exchange. All government organisations either are currently using the corporate environment or have plans to migrate to the corporate environment.

Government is just completing a major planning exercise to determine the appropriate architecture and implementation approach to employ in migrating its desktop and LAN assets to Windows 2000. The Windows 2000 Active Directory will be used to provide authentication and directory function for government's LAN and OIS environment. The architecture envisions that inwardly-facing LOB applications will also be integrated using the Active Directory.

With respect to LOB applications, the following application integration issues must be considered. To limit the impact that changes to LOB applications have on the installed desktop infrastructure, government is in the process of adopting a direction that all inwardly-facing LOB applications must be accessible through one of the following means:

1. Web Browser;
2. Windows Terminal Server session; or
3. Current "Mainstream" Desktop software releases and versions.

However, the focus of government LOB applications is changing from a predominantly inwardly-facing environment that supports government employees in their work. Many of the new applications being considered and planned are outwardly-facing to support direct interaction with citizens and businesses. Government has no control over the

computing or network configurations or capabilities of these constituents. Outwardly-facing government applications will be primarily Web Browser based.

5. LOB Application Platform Environment

Over time, government LOB applications have been implemented on a wide variety of application platforms, primarily those outlined in the table below. Government has designated that IBM OS/390, Microsoft Windows NT/2000 and UNIX are the strategic platforms to be used for new application deployment.

LOB Application Platform	Application Infrastructure Profile
Compaq Open/VMS	Primarily centrally managed. A number of major applications primarily based on Oracle RDB DBMS and written in Powerhouse.
Microsoft Windows NT/2000	A mix of central and distributed management. A number of new applications have been, or are being developed, using the government standard Oracle DBMS. The use of the transaction (MTS) and messaging (MSMQ) facilities offered by Windows DNA is being considered or adopted for a number of new applications. Some applications have been, or are being developed, using the native Windows API set while some are using the JAVA API set. A number of development tools have been used. IIS is the primary web server used. Current application integration initiatives are focused primarily on the Microsoft Commerce Server platform.
UNIX Compaq/Digital UNIX Data General DG/UX HP/UX IBM AIX NCR MP-RAS UNIX SUN Solaris	A mix of central and distributed management. The majority of new applications have been implemented in the UNIX environment using the government standard Oracle DBMS. These applications have either been based on packaged solutions (e.g. Oracle Financials, PeopleSoft, SAP) or custom developed often using Oracle Designer and Developer 2000. Some applications are being developed using the JAVA API set. A number of other development tools have been used. A mix of web servers are used (e.g. Oracle, Netscape, Apache). Currently, a mix of application integration platforms from different vendors are used (e.g. IBM, Oracle, Netscape).