Indian and Northern Affairs Canada

Internal Audit Report

Audit of
Comprehensive Integrated Document Management (CIDM)

Prepared by:
Audit and Assurance Services Branch

Project #08-19
December 2009

#2579891v14

Table of contents

Initialisms and Abbreviations

ADM	Associate Deputy Minister
AES	Audit and Evaluation Sector
CFO	Chief Financial Officer
CIDM	Comprehensive Integrated Document Management
FN	First Nation
GoC	Government of Canada
HQ	Headquarters
INAC	Indian and Northern Affairs Canada
LMRB	Litigation Management and Resolution Branch
RCM	Responsibility Centre Manager
TB	Treasury Board of Canada

Executive summary

The Comprehensive Integrated Document Management (CIDM) system is a mission-critical document management system for Indian and Northern Affairs Canada (INAC). In order to achieve the Department's information management objectives, the system must be used consistently by the Department, and information should be easily stored, secured and made available in support of operational and strategic activities.

Following a preliminary survey of Information Management/Information Technology applications, which identified the CIDM application as a high-risk system, an audit[1] was conducted to provide a high level of assurance that:

- Information is created, stored and managed in accordance with Government of Canada policies and standards; and that
- CIDM effectively supports business operations and processes.

The audit was conducted over the months of January to September 2009. Our work was based on a sample of four regions, and included interviews, document reviews and functional demonstrations provided in the selected regions.

Based on the findings from our audit, CIDM does not effectively support business operations and processes in a consistent manner, nor is information created, stored and managed consistently in accordance with relevant policies and standards. Inconsistencies in the interpretation, application and enforcement of policies were identified in a sample of regions, as well as inconsistencies in routine operating practices.

Information management is a critical component of knowledge management. Knowledge management systems should increase productivity, improve organizational responsiveness and competency, and stimulate and encourage innovation. Key concerns surrounding knowledge management include knowledge loss resulting from organizational changes and a retiring workforce, the obsolescence of technology, changes in formats and standards for storage and retrieval, and changes in business processes. These factors highlight the importance of knowledge management and CIDM as an information management solution to INAC.

The findings indicate that CIDM is not adequately managing information and is not supporting overall knowledge management for INAC. We recommend that the issues be addressed according to the recommendations presented. Furthermore, we recommend that the overall information management solution be re-evaluated in the context of knowledge management, with a focus on the efficiency of capturing and retrieving important information and on consistency of system performance across all regions.

[1] Our audit was executed in conformity with the Internal Auditing Standards of the Government of Canada. It does not constitute an audit or review in accordance with any Generally Accepted Auditing Standards (GAAS).

Summary of findings and recommendations

The table below captures a summary of the findings and recommendations contained within the report in the order in which they appear. Findings 1 through 6 relate to compliance with policies and directive requirements and findings 7 through 13 relate to system performance and effective support of business operations. The top three findings are the following:

- Security classification policy violations, which increases the risk of exposure to sensitive information by unauthorized personnel (i.e. Findings #2 and #3)
- Inconsistent performance and inability to easily retrieve documents in CIDM (i.e. Findings #5, #7, #9 and #10)
- Possible license infringement. There appear to be 837 more active CIDM users than allowed under the PWGSC contract (i.e. Finding #6)

Ref #	Findings	Recommendations
1	Lack of a defined retention and disposition policy for archiving electronic documents. In addition, an excessive amount of non-prioritized information is captured and stored in CIDM.	Define a retention and disposition policy. In particular, establish an appropriate retention and disposition schedule in consultation with Library and Archives Canada. An archiving solution should be designed in the interim and consistently followed across the regions and at headquarters. Introduce risk management techniques to identify and retain information that supports key management decisions or that becomes important when aggregated. Data capture in CIDM should align with an effective document classification policy.
2	Documents classified as Protected C or above are stored electronically in CIDM in violation of directive requirements[2].	Introduce an automated control to prevent users from storing Protected C and above documents electronically in CIDM.
3	Lack of user awareness surrounding document security classification. Document misclassification increases the chance of exposure of sensitive information to unauthorized individuals.	Perform periodic reviews to identify and correct document security misclassifications and establish an awareness program and user training related to document classification.

[2] Electronic Document Management Directive 2009

4	Inconsistent application of business rules and naming conventions across business units and regions. Lack of user awareness is preventing Department-wide adoption and use of business rules among INAC employees.	Establish a working group to define and articulate common and applicable business rules across the Department.
5	CIDM profile titles are not unique, which violates directive requirements[3]. Titles do not provide sufficient information to identify and retrieve documents efficiently.	Establish controls that force profile titles to be unique (e.g. an automatic search for the title in the database prior to allowing its use), as well as a policy to require profile titles to be descriptive with key reference numbers to assist in document identification and retrieval. The policy should be incorporated into an awareness program and user training.
6	Possible license infringement. There appear to be 837 more active CIDM users than allowed under the PWGSC contract.	Confirm number of users and review appropriate course of action to ensure compliance with licensing agreement.
7	Restrictive access rights are limiting users' abilities to view complete lists of searched documents.	Review system policies regarding access rights and perform risk-benefit analysis to validate access restrictions. These policies should align with security classification policies.
8	Lack of consistency and user awareness related to assigning iRIMS-generated file numbers to CIDM documents.	Implement an awareness program and user training to encourage consistent file numbering.
9	Inconsistent system performance across regions.	Conduct a review of systems and networks to identify factors affecting system performance and consider recommendations from the previous architecture review.
10	Protected C and above document profiles do not provide sufficient information for document retrieval.	Establish and enforce business rules, in conjunction with Recommendation #4, that require profile location fields to be descriptive and conducive to efficient document retrieval.
11	Lack of system performance monitoring.	Select performance metrics and establish benchmarks to be used for monitoring and measuring system performance across all regions.
12	Inability to easily access contents of libraries in other regions, which is causing document redundancies in system.	Conduct an assessment to determine the feasibility of integrating all departmental files into one corporate library that employees from all regions can access.

[3] Electronic Document Management Directive 2009

13	Lack of user awareness regarding CIDM benefits, objectives and technical matters due to insufficient communication.	Develop a communication strategy to address end-user misconceptions, communicate the program benefits and show progress against program objectives. A formal and consistent awareness and training program should be delivered in all regions and, upon delivery of the program, a process to monitor and measure compliance should be developed, instituted and enforced.

1. Background

INAC's significant investment in Information Management/Information Technology (IM/IT) serves to reach and support First Nations, Métis, Inuit, and Northerners, enable key strategic INAC programs and support operational business activities within the Department itself.

The Comprehensive Integrated Document Management (CIDM) system is an enterprise content management system. CIDM is the system name for INAC's use of Hummingbird Enterprise™ DM and Hummingbird Enterprise™ RM solutions. INAC extended their document management investment to include Hummingbird Enterprise™ Collaboration. Hard copies of documents such as correspondence to INAC are scanned using Hummingbird Imaging with Optical Character Recognition (OCR) to allow full-content searching.

The IM/IT Audit Universe report of December 2007 provided the Chief Audit and Evaluation Executive (CAEE) with knowledge of the overall IM/IT universe and the related risks involved. The IM/IT Audit Universe report identified data integrity, redundancy and legacy systems issues that could diminish the provision of high-quality information required for performance measurement, reporting and decision-making. A preliminary survey of IM/IT Applications was then conducted to identify the applications with issues and risks that would require further attention by INAC management. This preliminary survey of IM/IT applications identified the Comprehensive Integrated Document Management (CIDM) application as a high-risk system.

The 2009 Corporate Risk Profile identifies, as one of the department's top eight risks, information for decision-making. The profile categorizes this risk as INAC not making sufficient progress to improve access to timely, pertinent, consistent and accurate information to support planning, resource allocation and programming decisions, monitoring / oversight, and to fulfill its accountability obligation. CIDM, as part of the department's information management strategy, is expected to play a key role in this process by promoting the availability, timeliness and consistency of information for decision-making purposes.

CIDM is the INAC implementation of Records Documents Information Management System (RDIMS) and is a mission-critical document management system for the Department. The CIDM application is used to store official Departmental records and to meet the recorded information requirements of the Department. This application should facilitate the process of capturing, storing, organizing, sharing, retrieving, re-using, protecting and disposing of information in an electronic environment, regardless of format and without geographic or organizational barriers. The success of the system is based on the degree to which the organization uses the system consistently and the ease with which information is stored, secured and made available in support of operational and strategic activities.

The 1999 CIDM business case states that the objective of the initiative is to resolve serious and costly deficiencies in document and records management practices at INAC. A 2004 CIDM Renewal Project Presentation states the following annual cost savings, totalling $49.20M:

- 50% reduction in the time spent by office workers managing documents each week. Annual cost savings of $37M.
- 50% (25,000) of new documents not printed and stored as hard-copy. Annual cost savings of $6M.

- Reduction of printing or copying 25,000 documents per month. Annual cost savings of $5.4M.
- Floor space filing cabinet savings in Manitoba. Annual cost savings of $0.75M.
- Reduction of IT overtime in B.C. Annual cost savings of $0.06M.

The 2004 CIDM Renewal Project also summarized the benefits of CIDM to INAC experienced to date. Such benefits included operating cost savings, space savings, elimination of shared drives and 40% time savings in providing First Nations researchers with document access. In addition, the project discussed specific as well as generic process improvements resulting from the use of CIDM. These actual and perceived benefits were taken into consideration when performing the audit of CIDM.

2. Objective and scope of the audit

The objectives of this audit[4] are to provide a high level of assurance that:

- Information is created, stored and managed in accordance with Government of Canada (GoC) policies and standards; and
- CIDM effectively supports business operations and processes.

Further to consultation with INAC management, interviews were conducted in the regions of British Columbia (BC), the Northwest Territories (NT), Atlantic Canada (AT) and the National Capital Region (NCR). These regions were selected to obtain a nationwide perspective of the system. Vancouver (BC) and Ottawa (NCR) were representative of high-density office locations with a high level of system utilization and, in contrast, Yellowknife (NT) and Amherst (AT) were representative of smaller office locations with a low level of utilization and subject to bandwidth constraints.

The scope of the audit was to determine how CIDM supports effective and efficient operational processes across the Department.

The audit addressed the following broad areas:

- Information Creation - policy, practices and workflow to collect and get information into CIDM, including classification, completeness and validation closest to when information is first entered (ease of use, training and support documentation should also be addressed);
- Storage and Retrieval - for the consistency, completeness, accuracy of stored documents, and usefulness of the information as well as compliance to information security and other GoC standards and policies;
- Overall Information Management (IM) Oversight - the overall Information Management program as it relates to CIDM, including management oversight and management's enforcement of GoC standards; and
- IT risk management practices, including business continuity planning.

[4] Our audit was executed in conformity with the Internal Auditing Standards of the Government of Canada. It does not constitute an audit or review in accordance with any Generally Accepted Auditing Standards (GAAS).

The scope was further refined to centre on the following guiding principles. They were discussed and agreed to with INAC management based on the status of the system at the time of our audit:

- The audit would be based on a sample of regions, namely National Capital Region, British Columbia, Atlantic, and Northwest Territories;
- The audit of the business process, adherence to GoC policies and information management program was performed through interviews with the management team of INAC and of Regional offices; and
- The controls to review included workflow controls, IT-Dependant Manual (ITDM) controls and application controls related to information privacy and information security. Where applicable, we also reviewed compliance with GoC policies and, in particular, compliance to the Treasury Board Policy on Information Management.

Please note that the scope of the issues discussed in this report is based on a sample of regions and may not reflect conditions in all INAC regions. We make no guarantee that we have identified all of the issues related to the CIDM system, only those that we were able to identify during our audit.

3. Statement of assurance

Our objectives were to provide a high level of assurance that information is created, stored and managed in accordance with Government of Canada (GoC) policies and standards, and that CIDM effectively supports business operations and processes.

Sufficient work was performed and the necessary evidence was gathered to support the findings, recommendations and conclusions contained in this report.

Our work is based on a comparison of the conditions against pre-established audit criteria and sub-criteria agreed to by management. The criteria and sub-criteria are based on Control Objectives for Information and related Technology, version 4.1 (COBIT 4.1) and the Project Management Institute's Project Management Body of Knowledge (PMI PMBOK). Audit criteria are detailed in *Appendix A – Audit Criteria*.

In addition to the Internal Auditing Standards of the Government of Canada, our audit procedures were aligned with the Treasury Board *Policy on Internal Audit* and related policy instruments and International Standards for the Professional Practice of Internal Auditing.

For the purpose of this audit, the following definition of knowledge management (KM) was used:

> "Knowledge Management is the practice of selectively applying knowledge from previous experiences of decision making to current and future decision making activities with the express purpose of improving the organization's effectiveness."

The ultimate success of CIDM will depend on its ability to facilitate effective knowledge management for INAC. Leading research in knowledge management was used to guide the audit and support our findings and recommendations. The knowledge management framework and research are detailed in *Appendix B – Knowledge management criteria and research.*

4. Scope limitations

At the time of our audit, evidence to demonstrate the following was not made available:

- Reports and information to confirm the CIDM program has achieved and continues to achieve the return on investment (ROI) outlined in the management briefings and relevant CIDM documentation, including the following specific metrics:
    - Annual savings of $49M projected within two years;
    - Gain of five hours per employee, resulting in an estimated 25,000 hours of annual time savings; and
    - Reduction in average response time of Access to Information and Privacy (ATIP) requests from five days to 30 minutes.

  For our audit, the CIDM program refers to the following areas:
    - Operational activities;
    - Investment;
    - Systems comprising CIDM; and
    - Policy definition, implementation and enforcement.
- Reports on CIDM performance as experienced by end-users.
- CIDM Business Continuity Plan (BCP).

In addition, some testing could not be carried out in full. Specifically:

- Completeness of the CIDM database could not be established because there was no method of linking a document to a CIDM profile without knowledge of the CIDM number.
- Security clearance of all 39 people granted access to one or more of the sampled Secret documents could not be verified. While 37 people were confirmed to have Secret clearance, there were two people not found in the Security Services Information System (SSIS).
- The following tests could not be carried out because the documents could not be retrieved from their offline locations:
    - Accuracy of profile information; and
    - Existence (and accuracy) of prescribed retention period specifying storage location, media and disposition process.

Our audit of the CIDM system was based on inquiries of, and discussions with, INAC management, document reviews and functional demonstrations provided in the selected regions. We have not sought to confirm the accuracy of the data, information and explanations provided by management in all cases. Where possible, we used testing to validate information. Additional assessments may reveal further issues.

Our audit of the CIDM system was executed in conformity with the Internal Auditing Standards of the Government of Canada. It does not constitute an audit or review in accordance with any Generally Accepted Auditing Standards (GAAS).

5. Methodology

5.1 Temporal scope

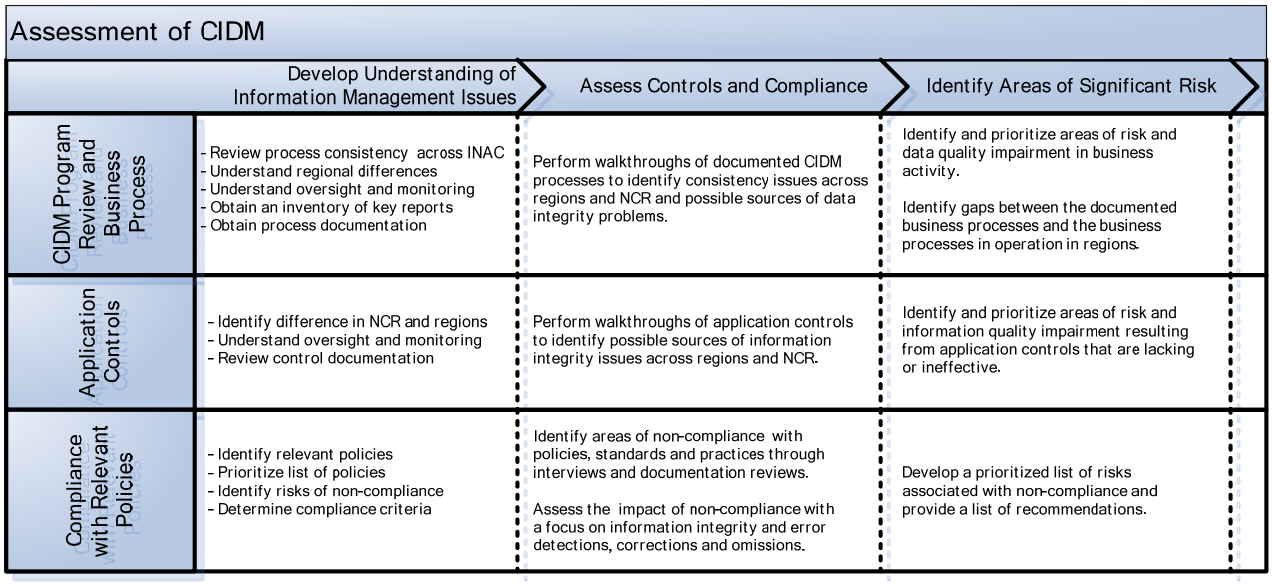
Our audit was conducted from January to September 2009. High-level planning activities were undertaken over the first two months to develop an understanding of the IM issues, and fieldwork was then performed from March through July 2009 to assess system controls and compliance to relevant policies. To validate information obtained through interviews and documentation reviews, testing was conducted from July to August 2009, and the final analysis and report development was completed in September 2009.

5.2 Audit approach

Four key areas were reviewed as part of our audit of CIDM:

1) CIDM program
2) Business process
3) Application controls
4) Compliance with relevant policies, practices and standards

The following diagram provides an overview of our audit and related key activities:



These are further described below.

5.2.1 CIDM program

Because proper program management is a fundamental pillar to a successful system, CIDM program documentation was used to identify key program management controls and develop process walkthroughs for the audit. The following high-level activities were undertaken:

- Reviewed CIDM program management documentation for evidence of the following components:
  - Overall strategy;
  - Resource plan;
  - Process to control design changes;
  - Stakeholder satisfaction;
  - Benefits realization; and
  - How the system is used.
- Identified process documentation gaps and conducted additional interviews and documentation reviews when possible.

5.2.2 Business process

The list of documents reviewed as part of this audit is included in *Appendix C – Documents reviewed.* The following high-level activities were undertaken as part of the business process review:

- Reviewed a sample of process controls, as documented by various business units, which we identified as critical to the success of the system. The process controls are intended to comply with relevant GoC standards and policies with respect to documentation management and retention. The review included testing a sample of documentation profiles, the use of standardized file numbering and reviewing CIDM business rules.
- Reviewed consistency in design and operating effectiveness of business process controls in a sample of regions, including NCR. The review was performed by examining the following:
  - Compliance to relevant policies such as the Records and Dispatch policy; and
  - Consistency of business rules across regions, within business units of any given region.
- Identified key reports generated by CIDM to support INAC operations.
- Highlighted process documentation gaps and requested (and conducted when possible) interviews and further documentation reviews to determine whether there were other compensating internal business controls not included in the documentation provided.

Thirty-two interviews with end-users, CIDM and regional management and INAC technical resources amplified the information reviewed in the CIDM documentation. The CIDM documentation was used to identify a set of key internal controls and develop process walkthroughs for the review. To better understand the existing CIDM system and its associated business process, the following activities were performed:

- Interviewed and conducted walkthroughs with representatives of the following groups in all four sample regions:
    - Executive Group;
    - Access to Information Group;
    - Human Resources Group;
    - Information Management Group;
    - Information Technology Group; and
    - Legal Services Group.
- Received functional demonstrations of the CIDM system from IM/IT representatives in each sample region.

The demonstrations provided further understanding of the application and the extent to which the business logic has been embedded into CIDM's functionality. Once knowledge was obtained regarding the previous business process and CIDM system, we were better able to identify the types of internal controls and behaviours that should be found in the current CIDM system.

5.2.3 Application controls

The adequacy of procedures and application controls was assessed within the context of the business processes that they support. Accordingly, a top-down, risk-based audit of the CIDM application was performed in coordination with the business process owner of the organization. The following high-level activities were performed:

- Assessed consistency of the application controls in place to identify, correct and report documentation management issues, including data classification, ownership, storage, retrieval and archiving;
- Assessed operating effectiveness of application controls across a sample of representative regions; and
- Assessed how the application controls support business processes.

To assess the application controls, we walked through the CIDM business process and reviewed the CIDM documentation, the CIDM training manual and its associated activity workflow, to develop a list of expected application controls.

5.2.4 Compliance with relevant policies, practices and standards

To assess CIDM compliance with relevant policies, practices and standards, the following high-level activities were performed:

- Identified and reviewed a prioritized list of relevant standards, directives, policies and practices based on a review of business process controls across regions. The list consisted of:
    - Business rules for CIDM and records management by region;
    - Procedures for adding and searching a CIDM document in WebCIMS;

- Procedures for inserting the CIDM document number and file name, and adjusting access controls to share documents;
- Procedures for saving Protected C and above documents in CIDM and removing the content of Protected C or above documents previously stored in CIDM;
- Standards for electronic documents as business records (e-records); and
- Guideline for email management.

- Assessed CIDM compliance to relevant INAC-specific standards, directives, policies and practices for information management. These included the following:
  - Directive for electronic document and email management as well as imaging of text based records;
  - Policy for INAC Information Management & Information Technology Governance;
  - Naming conventions and profiling guide for CIDM; and
  - Profiling conventions for CIDM.

5.3 Audit framework (COBIT, PMI PMBOK)

The audit framework was developed based on the Control Objectives for Information and related Technology (COBIT). COBIT is a set of leading practices for IT management created by the Information Systems Audit and Control Association (ISACA), and the IT Governance Institute (ITGI). COBIT provides managers, auditors and IT users with a set of generally accepted measures, indicators, processes and best practices to assist them in maximizing IT benefits and developing appropriate IT governance and control in an organization.

The audit criteria also included components of Project Management Institute's Project Management Body of Knowledge (PMI PMBOK).

Our audit was conducted in conformity with the Internal Auditing Standards of the Government of Canada. Our audit procedures were also aligned with the Treasury Board *Policy on Internal Audit* and related policy instruments and International Standards for the Professional Practice of Internal Auditing.

5.4 Understanding the business context of CIDM

As previously outlined, CIDM is an integral tool in facilitating knowledge management for INAC. CIDM consists of 17 libraries across the country with over 6,000 users and almost 6 million documents.

The main challenges for CIDM are to:

- Move (initially) from a paper-based environment to an integrated electronic records and document management solution;
- Improve the effectiveness of group and team activities that involve people from multiple geographical locations and time-zones, internal and external to the Department; and

- Change employee work habits and culture by adopting and taking full advantage of electronic records and document management and collaboration solutions.

While the main anticipated benefits of CIDM reside it its ability to:

- Share and retrieve information/documents between users and groups when working;
- Make finalized information/documents available to a large user community; and
- Facilitate the process of capturing, storing, organizing, sharing, retrieving, re-using, protecting and disposing of information in an electronic environment, regardless of format and without geographic or organizational barriers.

5.5 Testing methodology

We conducted tests focused on two main areas:

1) Profiling of Protected C or above documents in CIDM; and
2) Storage of Protected C or above documents in CIDM.

The testing was aimed at determining whether CIDM is being used consistently and in accordance with policy directives, and to assess the ease with which classified information is retrieved. The focus of the testing was on classified documents because they require a higher degree of management and control to maintain confidentiality, availability and integrity.

5.5.1 Profiling of Protected C or above documents in CIDM

The Electronic Document Management Directive specifies the following[5]:

" a) All unclassified, Protected A or Protected B electronic business documents must be stored within an approved electronic document management solution.

b) All Protected C, Confidential, Secret or Top Secret electronic business documents must be registered within an approved electronic document management solution and stored offline on a removable device that can be securely stored.

c) All online discussions hosted by INAC in support of departmental operations that provide context for policy or business decisions must be captured for storage within an approved electronic document management solution at the conclusion of the discussion.

d) All electronic business documents stored in an approved electronic document management solution must be assigned metadata values that provide business context for the record. The metadata elements must include:

i. A unique document / object title
ii. A document type designation to help with the evaluation of information
iii. The name of the contact responsible for the creation or collection of the document
iv. A link to the program function and activity for which the document was created to enable application of an appropriate record disposition authority.

[5] Electronic Document Management Directive 2009

v. *The technical application needed to access the information stored within the electronic document*

e) *All electronic business documents stored in an approved electronic document management solution must be assigned access controls appropriate to the protection and preservation requirements of the document / object content. "*

To assess whether the CIDM database was complete, a search in CIDM for a sample of Treasury Board (TB) Submissions was conducted. A list of TB Submissions for the period of 2006-2009 was obtained. All TB Submissions should be profiled in CIDM with appropriate classification in accordance with directives[6]. A random sample of 16 TB Submissions from a population of 156 was selected to test for database completeness.

The test for database completeness could not be carried out because there was no evidence of a process to link a CIDM profile for a TB Submission to the TB Submission number or control number. Therefore, it was not possible to determine whether TB Submissions are:

- Consistently saved in CIDM; and
- Profiled and saved in accordance with departmental policy.

We assessed compliance with directive requirements for document profiling in CIDM. Our focus was on documents with Secret classification because these documents are both easily identifiable and require a significant degree of management and control to maintain confidentiality, availability and integrity.

To test profiling compliance with directive requirements, we selected a random sample of 25 Secret documents. For each sample document, we verified that the following elements existed in the document profiles:

- A unique document/object title;
- A document type designation to help with the evaluation of information;
- The name of the contact responsible for the creation or collection of the document;
- A link to the program function and activity for which the document was created to enable application of an appropriate record disposition authority; and
- The technical application needed to access the information stored within the electronic document.

The security clearance of the authors and persons granted access for the 25 sample documents was also reviewed. A security check was done for the document authors, as well as individuals granted access to the document by the author, in order to assess whether access rights to classified documents in CIDM were appropriate based levels of security clearance.

Finally, we attempted to retrieve the 25 sample documents based on the information provided in the location field of the document profile, to assess the ease of retrieval of Protected C and above documents.

[6] Electronic Document Management Directive 2009, Record Keeping Directive 2009

5.5.2 Storage of Protected C or above documents in CIDM

The directive requirements specify that storage in CIDM for Protected C and above documents (i.e. Protected C, Confidential, Secret, and Top Secret) is prohibited. Protected C and above documents should be profiled in CIDM and securely stored offline on a removable device. The database was scanned for Protected C or above documents to assess adherence to the directive requirements.

To assess whether misclassified documents exist in CIDM, a search for Secret documents misclassified to be Protected B or below (that is, Protected B, Protected A, or unclassified) was conducted. A content search for key words "Memorandum to Cabinet", "Treasury Board Submission", "Secret", and "Top Secret" was conducted and a sample of 25 documents from the resultant list in the Atlantic (AT) region was selected for further review with the guidance of the system and security advisor for INAC.

Overall, the test results indicate that Protected C and above documents are not profiled and stored in compliance with directive requirements and that naming and profiling conventions are hampering system performance. The specific impacts of the results are incorporated into the findings and recommendations of the following section (specifically, Subsections 6.1.2, 6.1.3, and 6.2.2).

Testing limitations that impacted the scope of the audit were outlined in Section *2. Objective and scope of the audit* and are further discussed in Subsection 6.2.2. In particular, the inability to retrieve document samples prevented us from completing all test procedures. We also were unable to establish the security clearance of two of the 39 individuals tested because they were not found in the SISS system by INAC personnel.

6. Findings and recommendations

6.1 Compliance with relevant policies and standards

The result of the procedures described in Section *5. Methodology* is that we cannot confirm with a high degree of assurance that information is created, stored and managed in accordance with GoC policies and standards.

The findings that substantiate the above statement relate to:

1) Retention and disposition;
2) Security level infringements and misclassifications;
3) Business rules and naming conventions;
4) Leading practices and recommendations from previous reviews; and
5) Licensing infringements.

The supporting findings are outlined below.

6.1.1 Retention and disposition

A lack of consistency in interviewee responses indicates that the Department does not have a retention and disposition policy and/or employees are unaware of such policy. We asked INAC officials for a copy of the CIDM retention and disposition policy document; however, officials could not locate such a policy for our audit. Therefore, we cannot confirm that a retention and disposition policy has been established and/or made available to CIDM users. Nor can we confirm that such a policy is in accordance with, and has the approval of, Library and Archives Canada (LAC).

LAC provides authority for records disposition to government institutions through one of its two Records Disposition Authorities (RDAs):

- Multi-Institutional Disposition Authorities (MIDA): Relate to records managed by all or a multiple number of government institutions, and allows the institutions to dispose of records under certain terms and conditions; and
- Institution Specific Disposition Authorities (ISDAs): Relate to records managed by a single government institution, and allows the institution to dispose of their records under certain terms and conditions. ISDAs take precedence over all other RDAs issued by LAC. [7]

Authority to dispose of information is delegated by LAC through approved retention and disposition schedules. During our review in the sample regions, there was no evidence of any policies or procedures for the disposal of information in CIDM. As a result, INAC lacks the capability to dispose of material according to LAC schedules and is, therefore, in contravention of the *Policy on the Management of Government Information* and the *Library and Archives Canada Act*[8].

As outlined in *Appendix B – Knowledge management criteria and research,* the following key factors should be considered when implementing a knowledge management (KM) system such as CIDM:

- Structure;
- Culture;
- Task;
- Information and decision process;
- People; and
- Reward system.

While structure, tasks, information and decision processes, and people were addressed in various aspects of the CIDM system, there was no evidence to demonstrate an attention to culture or the design of appropriate reward systems, which requires setting the correct tone at executive levels of the Department.

---

[7] "Best Practices - Record Retention and Disposition Processes." Government of Canada. 7 July 2009. http://www.tbs-sct.gc.ca/atip-aiprp/isa-eer/isa-eer06-eng.asp.

[8] "Explanatory Notes for the Privacy Protection Checklist." Treasury Board of Canada Secretariat. 25 August 2010. http://www.tbs-sct.gc.ca/atip-aiprp/tpa-pcp/tpa-pcp10-eng.asp.

Evidence was also not available to demonstrate risk management techniques are used to identify important information worth saving. We observed an overabundance of information, the value of which is at times marginal, if not negative. This excessive capture of low-value documents forces users to lose valuable time sifting through files of data, a problem known in the industry as "data smog" (*Appendix B – Knowledge management criteria and research).*

In summary, effective KM is hampered by the lack of:

- Risk management techniques to identify important information worth retaining;
- A well-defined retention and disposition policy;
- A unified interface to the multiple regional CIDM libraries;
- Standardized practices to capture document profiles (used for document searches);
- Consistent practices for providing logical access; and
- User confidence in the system.

- Finding 1: Lack of a defined retention and disposition policy for archiving electronic documents. In addition, an excessive amount of non-prioritized information is captured and stored in CIDM.

- Recommendation 1: Define a retention and disposition policy. In particular, establish an appropriate retention and disposition schedule in consultation with LAC. An archiving solution should be designed in the interim and consistently followed across the regions and at headquarters. Introduce risk management techniques to identify and retain information that supports key management decisions or that becomes important when aggregated. Data capture in CIDM should align with an effective document classification policy.

A properly formulated retention schedule will prevent the accumulation of obsolete and transitory records and promote the availability and use of electronic records for appropriate periods of time. It will also make more efficient use of electronic storage media.

6.1.2 Security level infringements and misclassifications

Through our testing of compliance with directive requirements, we found Protected C and above documents stored in CIDM in violation of the Electronic Document Management and Record Keeping directives. We also identified several misclassified Secret documents stored in CIDM under Protected B, Protected A, and unclassified security levels.

A Crystal report listing all Protected C and above documents stored electronically in CIDM was generated on 1 June 2009, identifying one Protected C or above document. Another Crystal report was generated on 29 June 2009 identifying two Protected C or above documents, and a third Crystal report was generated on 26 August 2009 listing six Protected C or above documents. The electronic storage of classified information violates directive requirements[9] and poses a risk to the Department due to the sensitive nature of classified documents.

[9] Electronic Document Management Directive 2009

- Finding 2: Documents classified to be Protected C or above are stored electronically in CIDM in violation of directive requirements[10].

- Recommendation 2: Introduce an automatic control that prevents users from storing Protected C and above documents electronically in CIDM.

In addition to the directive requirement violations, misclassified Secret documents were found stored in CIDM. A key-word content search ("Secret", "Top Secret", "Memorandum to Cabinet", and "Treasury Board Submission") in the Atlantic region was conducted and a sample of 25 documents from the resultant list was taken for further review. Of the 25 sample documents, 15 documents were Treasury Board Submissions or Memorandums to Cabinet that should have been classified Secret.

In the sample of 25, eight documents labelled Protected A, four documents labelled Protected B, and three unclassified documents were confirmed to be Secret documents by the INAC security and system advisor due to their nature and content. Therefore, their storage in CIDM is a violation of policy and increases the chance of exposure of sensitive information.

- Finding 3: Lack of user awareness surrounding document security classification. Document misclassification increases the chance of exposure of sensitive information to unauthorized individuals.

- Recommendation 3: Perform periodic reviews to identify and correct document security misclassifications and establish an awareness program and user training related to document classification.

6.1.3 Business rules and naming conventions

During our site visits, we noted that business rules and naming conventions varied with region and business unit. Documentation to demonstrate that regions had established business rules and naming conventions was available for review; however, interviewee responses revealed that users were unaware of how to properly apply the established naming conventions and business rules. Interviewees noted that, as a result of this, they had difficulty locating files that had been stored in CIDM.

We also observed users profiling all their documents to the file number 9999-1. This number is the dedicated area for storage of personal files. When asked about this, users explained that their profile defaults were set to save documents to the file number. After consulting the CIDM business rule document, we observed the following under Personal Documents (non-work related) Section:

- 4.1. Personal documents allowed in the CIDM repository;

[10] Electronic Document Management Directive 2009

- 4.3. File classification number 9999-1 available for personal documents. (This number not to be set as personal profile default setting by end users); and
- 4.4. Personal documents deleted upon employee departure.

Naming conventions and business rules for knowledge management are paramount for good design and development practices in any organization. Capture and standardization is fundamental in supporting complex operations such as those of INAC. Business rules standardization is a core element of the automated infrastructure of any organization.

- Finding 4: Inconsistent application of business rules and naming conventions across business units and regions. Lack of user awareness is preventing Department-wide adoption and use of business rules among INAC employees.

- Recommendation 4: Establish a working group to define and articulate common and applicable business rules across the Department.

The document profile titles were found to be inconsistent and several documents in CIDM were observed to have single-character title fields (such as a digit or a '>' symbol). While the title is a mandatory field in the document profile, it suffices to enter in a space character, leading to a blank title field. While there is a documented CIDM naming convention, it is not consistently adhered to. As a result, numerous titles in the CIDM database do not provide any description of the document.

Due to the lack of descriptive titles with document reference numbers in CIDM, one cannot determine whether a document is profiled or stored in CIDM. This deficiency leads to the possibility of one document being stored multiple times under different titles; in addition, there is no method of establishing database completeness.

An automatically generated CIDM number prevents multiple instances of the same CIDM number in the database. However, there is no control in place to prevent multiple instances of a given title. It is possible to save two documents under the same title in CIDM and there were multiple documents titled "RESUME" and "COVER LETTER" found in the CIDM database.

- Finding 5: CIDM profile titles are not unique, which violates directive requirements[11]. Titles do not provide sufficient information to identify and retrieve documents efficiently.

- Recommendation 5: Establish controls that force profile titles to be unique (e.g. an automatic search for the title in the database prior to allowing its use), as well as a policy to require profile titles to be descriptive with key reference numbers to assist in document identification and retrieval. The policy should be incorporated into an awareness program and user training.

[11] Electronic Document Management Directive 2009

6.1.4 Leading practices and recommendations from previous reviews

A 2007 CIDM architecture review contained the following recommendations to "address performance issues, enhance functionality and ensure proper monitoring of CIDM":[12]

" 1. It was suggested by the manufacturer to implement Oracle Multi-Threaded Server (MTS). It is believed that this configuration will help alleviate the Oracle session limitation.

2. *Review virus scan policies to see if they can be modified on CIDM servers and all workstations. It is recommended that scan on write be enabled and scan on read be disabled. On the CIDM index server, the index location (C:\hummingbird) should also be excluded for both read and write. On the CIDM Webtop, it is recommended that the Webtop directory be excluded from read scan.*

3. *Monitor for table scans occurring within the CIDM database. Table scans themselves are not an indication of a problem but when a table has been designed with index, users performing searches against this table should not cause excessive table scans during these searches. If indexes are in place for these user searches, a resulting table scan will indicate issues with table indexes.*

4. *Review validity of the custom triggers, scripts and stored procedure to confirm their continued requirements. Some of these were designed with Docsopen in mind and may not be required with DM.*

5. *Grant remote desktop capabilities to your CIDM administrators. With this ability, they can be more proactive in monitoring the CIDM servers. Two examples would be to monitor cache counters to see how the DM servers are performing and monitor indexer errors while full text indexing documents to confirm the stability of the index.*

6. *INAC should consider migrating to LivelinkECM eDocs RM instead of Livelink iRims. This module is fully integrated to DM and the client component is a thin client unlike Livelink iRims, which is a fat client and requires an ODBC connection. This would significantly increase CIDM's reliability and responsiveness and overall client satisfaction.*

7. *The Corel Office suite should be replaced with the MS Office suite. The MS Suite has a tried and true ODMA compliant integration that would eliminate the interceptor requirements of Corel. This, in turn, would eliminate the requirement to automatically start CIDM on all workstations.*

It is also suggested the following be reviewed.

1. *Modify search profile by removing the filter lookup on Typist. Instead, put this filtered lookup on the profile entry forms for Author. The filter will only display users that are allowed to login. This filter should not be on the search form since a user may require searching for information created by a retired INAC employee. By putting the filter on the Author field of profile entry forms, only current employees can be selected as the Author.*

[12] CIDM Architecture review

2. *Produce a generic CIDM installation guide. The guide provided for review was an upgrade guide, not an installation guide. This guide is a requirement for any disaster recovery plan. This guide should be updated as required whenever a change in the server configuration changes (like an updated operating system).*

3. *Consider function based indexes. This would provide case-insensitive searching which would enhance the user experience.*

4. *Review disaster recovery plan and confirm all aspects of CIDM are considered. If a business continuity plan exits at INAC, CIDM must be considered as it can be used to provide quick access to required documentation.*

5. *Review items identified in RED in the CIDM Survey Result.xls file. Items in RED need attention.*

6. *Review all DCOM settings. Some settings were not present at all (such as security limits). Having consistent settings helps eliminate possible connection issues within/between libraries and communication issues between workstations and CIDM servers. CIDM relies on DCOM communication and these settings need to be configured correctly for CIDM to operate properly.*

7. *Review why the document type lookup has a filter on Groupfilter. This is not a standard column in this table and is affecting the maintenance of document types. This was experienced in the Library Maintenance tool while reviewing the development library provided to us for our use. We were not able to confirm whether this existed in the production library. We are presuming that the development environment is an exact duplicate of the production environment."*

We have not been provided evidence to demonstrate that the majority of the above recommendations have been implemented. This finding is supported by an email provided to us by the CIDM IT Team Lead

We did not conduct a detailed review of the recommendations as listed in the noted report.

6.1.5 Licensing infringements

The 14 March 2008 contract with Public Works and Government Services Canada (PWGSC) provides for 5,200 user licenses for the agreement term of 1 April 2008 to 31 March 2011[13]. No evidence of an amended contract was made available during our audit.

We were provided with a count of total documents and users by region on 4 June 2009, as seen in Table 1. We are unable to confirm the accuracy of these figures.

[13] RDIMS / RDIMS Protected B Licenses, Maintenance and Support, RA 4157

Table 1: Documents and Users by Region

Region	Total Docs	Percentage of Total Docs	Active CIDM Accounts From AD	Percentage of Total CIDM Accounts
*NCR	1506144	25%	3310	55%
*IM	25315	0%	90	1%
AB	602577	10%	238	4%
AT	258605	4%	145	2%
*BC	1101893	19%	413	7%
IOGC	151701	3%	88	1%
MB	602028	10%	264	4%
NU	304960	5%	97	2%
NT	245516	4%	366	6%
*ONS	24619	0%	440	7%
*ONN	247562	4%	See above	See above
QC	572547	10%	222	4%
SK	206259	3%	247	4%
YT	68967	1%	117	2%
Total	5918693	100%	6037	100%

*** approx number of active CIDM accounts due to library sharing**

While there are 5,200 licenses, there appear to be 6,037 active CIDM user accounts.

- Finding 6: Possible license infringement. There appear to be 837 more active CIDM users than allowed under the PWGSC contract.

- Recommendation 6: Confirm number of users and review appropriate course of action to ensure compliance with licensing agreement.

6.2 Effectively supporting business operations and processes

The result of the procedures described in Section *5. Methodology* is that we cannot confirm with a high degree of assurance that CIDM consistently and effectively supports business operations and processes.

The findings that substantiate the above statement relate to:

1) Access rights;
2) System performance;
3) Performance monitoring;
4) Library access and redundancy;
5) Achievement of program objectives;
6) Proactive communication; and
7) Effective knowledge management.

The supporting findings are outlined below.

6.2.1 Access rights

Many of the users interviewed complained of their lack of ability to view a complete list of CIDM stored documents when performing a search. Users believed that this lack of ability was due to limited access privileges associated to their CIDM account, meaning that a document matching a specific search criteria entered by the user may not appear as a search result because he/she does not have the appropriate access privilege. The user is, therefore, unaware that the document exists in CIDM. Because of this system characteristic, many users are losing trust in CIDM's ability to generate a complete list of documents based on given search criteria.

- Finding 7: Restrictive access rights are limiting users' abilities to view complete lists of searched documents.

- Recommendation 7: Review system policies regarding access rights and perform risk-benefit analysis to validate access restrictions. These policies should align with security classification policies.

User buy-in is essential to the success of an enterprise knowledge management system. An important aspect of knowledge sharing is obtaining high-quality knowledge and maintaining its excellence. Lack of trust in CIDM's ability to provide a complete list of documents is a barrier to its success as an effective knowledge management tool.

Additionally, during our regional interviews, we were informed of diverse practices when choosing a file number for documentation stored in CIDM. CIDM is integrated with Integrated Recorded Information Management System (iRIMS) and CIDM file numbers are generated by iRIMS. While file numbers are system-generated through iRIMS, the CIDM user has the option of choosing a file number from a fixed sample provided by iRIMS. Choosing the correct file number is the basis upon which the Records and Dispatch policy is triggered. Incorrect or inconsistent file numbering will lead to non-compliance and hamper efforts to locate and retrieve information.

- Finding 8: Lack of consistency and user awareness related to assigning iRIMS-generated file numbers to CIDM documents.

- Recommendation 8: Implement an awareness program and user training to encourage consistent file numbering.

6.2.2 System performance

Throughout our interviews, we often heard that system performance was a major issue. Functional demonstrations provided in all visited regions revealed that system performance differs from region to region. We observed particularly slow search response times in the BC regional office. Interviewees of that region complained of search response times averaging 1.5 to 3 minutes to display results. Users attributed

this delay to server speed. It can also be noted that the BC region has a high volume of both users and documents, as seen in Table 1, in comparison with the AT and NT regions.

- Finding 9: Inconsistent system performance across regions.

- Recommendation 9: Conduct a review of systems and networks to identify factors affecting system performance and consider recommendations from the previous architecture review.

We also assessed the ease with which Protected C and above documents are retrieved from off-line locations. The location field was reviewed in the profiles of 25 sample documents. The following observations were made:

- The location field was blank for 13 documents;
- The location field contained a comment (but not a location) for seven documents; and
- The location field contained a code or description for the remaining five documents, but the information was insufficient to describe the document's location.

As a result of the fact that none of the documents could be retrieved based on the profile information, requests for the documents were made to the document trustees. A window of five business days was given to establish document location, which we considered to be a reasonable turn-over period. The 25 sample document locations could not be retrieved from the trustees in five business days. Furthermore, there was no evidence to suggest that the documents could eventually be located. The inability to retrieve classified documents is a significant operational issue.

- Finding 10: Protected C and above document profiles do not provide sufficient information for document retrieval.

- Recommendation 10: Establish and enforce business rules in conjunction with Recommendation #4 that require profile location fields to be descriptive and conducive to efficient document retrieval.

6.2.3 Performance monitoring

According to the CIDM IT Framework Manual, the CIDM team is responsible for running monthly statistic reports and running scripts to generate statistical data for all regions. While we saw evidence of a CIDM server availability report, there was no evidence of reporting on performance experienced by end users.

The electronic document management directive, the imaging text-based business record directive and the record keeping directive all require that compliance reports be submitted to the Chief Information Officer (CIO) as well as Responsibility Centre Managers (RCMs). These reports would confirm the adherence to the appropriate standards. The following data points would be reported on:

- Ratio of active accounts within CIDM to staff with pre-defined groups;
- Number of documents filed within CIDM by business group;
- Identification of individual account holders that are not:
    - Adding to the collection

- Using metadata effectively

- Size of individual email accounts in use;
- Number of email messages filed within CIDM by account holder;
- Volume of paper records received within each region;
- Volume of scanning activity within each region;
- Volume of paper filing carried out within each region;
- Growth activity related to the capture of electronic documents added; and
- Growth activity related to file/volume creation (iRIMS component).

We could not find evidence that these data points were made available for review by the current CIO, nor if action was taken on unplanned performance variations. Furthermore, due to lack of evidence, we were unable to determine what analysis is performed and what action is subsequently taken as a result of the analysis.

- Finding 11: Lack of system performance monitoring.

- Recommendation 11: Select performance metrics and establish benchmarks to be used for monitoring and measuring system performance across all regions.

Reporting is essential to the improvement of a business application. It is important that performance reports are prepared, analyzed and acted upon on a timely basis. It is important for INAC to select performance metrics and establish benchmarks to be used for monitoring and measuring CIDM system performance across all regions.

6.2.4 Library access and redundancy

A leading practice of knowledge management is to establish a single access point to a repository of organizational corporate knowledge.

According to interview responses, INAC has separate libraries in every region. Users in one region, with access to their respective regional libraries, do not have access to documents located in other regional libraries. This separation becomes a problem when a CIDM document reference is placed in an email that is sent from headquarters to several recipients across different regions because these recipients are unable to access the CIDM document. As a result, entire documents are attached to emails causing additional network usage, CIDM duplication (when this document is received by the users and saved in their respective libraries) and inefficient use of a document management tool.

- Finding 12: Inability to easily access contents of libraries in other regions, which is causing document redundancies in system.

- Recommendation 12: Conduct an assessment to determine the feasibility of integrating all departmental files into one corporate library that employees from all regions can access.

Establishing a single access point to an integrated repository of corporate knowledge would eliminate duplication across regions and make documents easier to locate and access. A single access point would also improve the efficiency of IT infrastructure already in place.

6.2.5 Proactive communication

Based on numerous interviews in the regions, there is inconsistent training provided across the regions. During these interviews, we heard many different views of what people thought CIDM actually consisted of, what people believed was possible within the system and how best to create, store and retrieve information. We also heard diverse opinions on whether the system is available and functional. Some people felt it crashed often, while others felt the environment was stable and available most of the time. The primary reason for this perception is that the CIDM client, which end-users use to access the server, is known to have integration issues with iRIMS. During one of the regional demonstrations of CIDM, we witnessed the client crashing as soon as the end-user (who happened to be a technical CIDM lead for that region) tried to select a file number through iRIMS. Many end-users were not aware that this is a known issue.

IM/IT has metric reports showing that CIDM availability is near 99% on average, which suggests that the perception that CIDM crashes often might be attributable to the CIDM client crashing.

Evidence of communication to end-user communities highlighting the following was not made available for review:

- CIDM benefits;
- Current progress against ROI and CIDM program objectives;
- Known technical issues; and
- Performance differences between the client software and the main CIDM system.

In addition, there was no evidence to demonstrate that issues undermining end-user perception are captured, tracked, validated and addressed.

- Finding 13: Lack of user awareness regarding CIDM benefits, objectives and technical matters due to insufficient communication.

- Recommendation 13: Develop a communication strategy to address end-user misconceptions, communicate the program benefits and show progress against program objectives. A formal and consistent awareness and training program should be delivered in all regions and, upon delivery of the program, a process to monitor and measure compliance should be developed, instituted and enforced.

7. Conclusion

The objectives of this audit were to provide a high level of assurance that CIDM effectively supports business operations and processes and that information is created, stored and managed in accordance with Government of Canada policies and standards.

Based on information gathered through reviews of INAC documentation, interviews with INAC staff, and system testing, we could not confirm with a high degree of assurance that information is created, stored and managed in accordance with relevant policies and standards, nor that CIDM consistently and effectively supports business operations and processes.

Issues were identified pertaining to compliance with policies and standards, including a lack of a retention and disposition policy for archiving documents, security level infringements and misclassifications, inconsistent business rules and naming conventions, license infringements, and no evidence to demonstrate that recommendations from previous reviews were implemented and that leading practices are being followed.

Findings pertaining to the effective support of business operations and processes were also identified. Namely, there is a lack of user awareness due to insufficient communication, user trust is limited due to system access limitations, performance is inconsistent, classified documents are prohibitively difficult to retrieve, and there is redundancy across libraries. In addition, there is a lack of system performance monitoring, and it is not clear that the stated benefits of CIDM have been achieved.

The issues identified indicate that CIDM is not providing adequate information management and is not supporting overall knowledge management for INAC. We recommend that the issues be addressed according to the recommendations presented, which includes responding to previous recommendations.

Furthermore, in order to achieve effective information management and facilitate successful knowledge management, we recommend that CIDM be re-evaluated in the context of knowledge management, with a focus on the efficiency of capturing and retrieving important information and on consistency of system performance across all regions.

8. Management Action Plan

This document has been created in order to respond to the observations and recommendations of the internal audit of Indian and Northern Affairs electronic document management system, which is referred to as "CIDM" – Comprehensive Integrated Document Management.

BACKGROUND OF AUDIT:

In 2009, the Audit and Assurance Services Branch, of INAC's Audit and Evaluation Sector (AES), conducted an internal audit of INAC's utilization and configuration of the Government of Canada's electronic document management system (RDIMS)[14].

The audit concluded that it could not be confirmed with a high degree of assurance that a) Information in CIDM is created, stored and managed in accordance with relevant policies and standards, and b) CIDM consistently and effectively supports business operations and processes.

CONSULTATION:

The creation of the Management Action Plan for the Audit of CIDM was a collaborative effort across INAC. The plan was validated with all Regional Directors of Corporate Services, who are responsible for CIDM utilization and user support within each Region. Input was garnered via a site visit to Amherst, Nova Scotia which included discussions with the Director of Corporate Services, IM and IT support staff and users. Dialogue and input was also solicited from three external senior IM consultants and was presented at the Directors of Funding Services workshop in early 2010. Internal consultations were undertaken with INAC's IM and IT service provisioners, senior directors and the Chief Information Officer (CIO).

GOVERNMENT OF CANADA POLICY:

INAC's installation of the Government of Canada endorsed electronic document management system (RDIMS) ensures compliance with both Treasury Board (TB) and INAC's Information Management Policies and Directives. The TB IM policy suite dictates that "Deputy Heads are responsible for ensuring electronic systems are the preferred means of creating, using and managing information." Its use is essential in INAC meeting its obligations under E-discovery and ATIP, as well as over 10 Government of Canada Acts (including, but not limited to the *Canada Evidence Act*, the *Copyright Act*, the *Library and Archives of Canada Act* and the *Security of Information Act*).

[14] This COTS (Commercial Off The Shelf) solution is installed across the department, and is internally referred to as "CIDM" – Comprehensive Integrated Document Management. It is supported by central agencies (LAC, TBS and PWGSC) through senior level committees and user groups. The vendor is OpenText (a world leader in electronic content management solutions), who holds the current contract for the Government of Canada electronic document management system, working closely with PWGSC on behalf of all Government of Canada departments and agencies.

ELECTRONIC DOCUMENT MANAGEMENT AT INAC

Every new user (employees and consultants) receives three hours of mandatory training on the use of CIDM, plus a one hour desk visit by a highly experienced "power user" to assist in personalization. Approximately seven hundred users are trained on CIDM each year.

INAC'S configuration of RDIMS has been slightly modified to co-exist with Groupwise (the department's standard email platform), and the Microsoft Office suite, but it is deemed to be a standardized environment for security patches, upgrades, etc. CIDM is the official document repository of the FNITP system (automated profiling, limited access) and it allows INAC to cap email storage requirements, thereby reducing costs and traffic on the network

While the application has been installed and training has been provided to all INAC employees, there are still opportunities to further integrate RDIMS principles and practices into departmental activities and business processes. Consistent with the key audit findings, RDIMS was not implemented smoothly within INAC nationally. Additional measures to ensure its proper use to collectively manage electronic information within the specific business environments are still required to be coordinated and monitored by IMB (Information Management Branch).

KEY AUDIT FINDINGS

The audit findings can be broken down into seven key observations which are identified below, along with IMB's chosen approach towards continuous and ongoing improvement.

1. User Awareness:

Observation: There exists a lack of user awareness surrounding appropriate document classification, user responsibilities and support, and the benefits of prioritizing this activity.

Action: INAC's IMB will embark on a re-invigorated approach to change management and governance to minimize the knowledge gap as it relates to system usage. More effort will be concentrated on persistency of uptake, including endorsement/enforcement by senior management. In the short term, IMB will conduct a series of user forums and surveys to garner input and suggestions from departmental employees on where they see specific areas of improvement being required.

Planned Implementation Date: (September 2010)

2. Retention and Disposition

Observation: INAC's standardized retention and disposition policies are not being consistently followed across the department.

Action: IMB will work with the Regions and program areas to ensure that existing Retention and Disposition Authorities (RDA's) are applied consistently to CIDM document collections. This work will be conducted in parallel with departmental activities currently underway with Library and Archives Canada (LAC) on updating many of the existing RDA's.

Planned Implementation Date: (December 2010)

3. Business Value of Information

Observation: CIDM's mandatory save environment is leading to an overabundance of transitory materials being captured and stored.

Action: IMB will develop a strategy which focuses on identification of business versus transitory materials, which will include the identification of an appropriate storage facility for transitory records. Also, IMB will lead in the development of an enterprise search strategy which can comb all departmental repositories in support of ATIP and e-Discovery.

Planned Implementation Date: (December 2010)

4. Document Security

Observation: Confusion exists within the department around appropriate document security protocols, profiling and business rules.

Action: Since the conclusion of the audit, IMB and the Security and Occupational Health and Safety Division (SOHSD) have partnered together in an effort to better educate, measure and monitor the handling of electronic documentation. To that end, steps have been taken to include more frequent messaging around appropriate document security levels. In particular, changes have been made within the CIDM training curriculum to aid users in better identifying appropriate document security designations.

Over the long term, IMB will continue to partner with SOHSD to further improve education, measurement and monitoring of the handling of electronic documentation.

Planned Implementation Date: Immediate and ongoing

5. Naming Conventions and Profiling

Observation: There exists inconsistent application of naming conventions and access controls.

Action: In the short term, IMB will educate and clearly disseminate to the Regions INAC's best practices and standards as they relate to naming conventions, while at the same time promoting more openness within the document access controls. This will be measured through IMB's Regional and Sectoral Scorecarding exercise on an ongoing basis.

Planned Implementation Date: (September 2010 and ongoing)

6. Performance

Observation: Improvements should be made in the measurement, monitoring and remediation of CIDM performance and response times.

Action: IMB will establish and coordinate a national review process in collaboration with Regional service partners to identify factors affecting system performance. Once this process has been established, IMB will lead in the ongoing measurement, monitoring and remediation of performance and response times across all Regions.

Planned Implementation Date: (September 2010 and ongoing)

7. Licensing

Observation: There were at the time of the audit, more active users than actual licenses.

Action: Since the conclusion of the audit, IMB has remitted to PWGSC the required dollars to cover the identified gap.

In the medium term, IMB will apply more rigour around licence management. The anticipated approval of the departmental Entry/Exit project will dramatically assist in this regard.[15]

Planned Implementation Date: (December 2010 and ongoing)

[15] The proposed departmental Entry/Exit project is a multi-jurisdictional initiative which will allow for the identification of individuals both coming into, and leaving, the department at all times. This will result in more rigour around physical security, IT security, finance, accommodations, payroll, asset control and software licensing.

FUTURE DIRECTION OF RDIMS

Over the medium to longer term (12 to 18 months), a new electronic document management system is planned for implementation within INAC. This new version (Enterprise Content Management – ECM) will be the Government of Canada endorsed solution to replace the existing RDIMS product. It is further anticipated that support and updating to CIDM will cease prior to 2013. INAC is a member of the RDIMS Lifecycle Working Group, ensuring that the department stays abreast of current developments, as well as having input into the business requirements of the new product. IMB (with Regional input) has developed a business case to move to the next iteration, which will address many of the shortcomings within the current system ("Looks old, acts old.") including folder "drag and drop" functionality and auto-profiling.

The focus of IMB's approach to the new iteration of RDIMS will include significant attention being paid to user needs, requirements and awareness. It is important to note that the investment in change management linked to this initiative will be on par with the level of resources attributed to the technical configuration. The interfaces and system logic have been updated by OpenText to better reflect today's systems' look, feel and function (as one example, "Drag and Drop" functionality has been introduced).

Another key factor in this equation is that INAC is in the midst of IM Policy Suite Renewal, which will be leveraged to include better direction, instruction, guidance and clarity where ambiguity from a user perspective exists. The 2010-2015 IM/IT Strategy is in late draft, with expected release in spring 2010.

A Five-Year Information Management Strategic Plan and Five-Year Year IM Action Plan (covering 2010 to 2015) was recently approved by the CIO, which identifies tangible actions which will also assist in the further development and maturation of INAC's Information Management program.

Appendix A – Audit Criteria

1. Business Process
    a. Gain reasonable assurance that the business process associated with the CIDM system has been defined and documented.
    b. Gain reasonable assurance that the requirements for the CIDM system, including any required application controls have been documented and provided to IT representatives.
    c. Gain reasonable assurance that the business processes have been designed with appropriate controls to manage the risks associated with the business process.
    d. Gain reasonable assurance that the business process, including the new system, has been designed to include appropriate automated preventive controls.
    e. Gain reasonable assurance that the business process has been designed to support detective control activities, such as monitoring.
    f. Gain reasonable assurance that the application controls appropriately support the intended business process.
    g. Gain reasonable assurance that a risk management plan has been developed and that tools and technologies are in place to effectively support risk management activities.
    h. Gain reasonable assurance that a formal training plan has been established to support the proper use of the system.
    i. Gain reasonable assurance that the key reports produced effectively support INAC operations.

2. Adherence to Government of Canada policies
    a. Gain reasonable assurance that the CIDM system creates, stores and manages information in accordance with relevant Government of Canada policies.
    b. Gain reasonable assurance that CIDM is in compliance with relevant Government of Canada risk management policies.

3. Information Management Program
    a. Gain reasonable assurance that an overall strategy document has been developed to define the vision and direction for CIDM. The objectives must be aligned to those of the portfolio of the organization.
    b. Gain reasonable assurance that an appropriate resourcing plan has been developed, approved and communicated to required parties.
    c. Gain reasonable assurance that the overall Information Management program as it relates to CIDM including management oversight and support and management's enforcement of GoC standards is appropriate.

d. Gain reasonable assurance that a robust process exists to control design changes, including responsibilities, forms, procedures, reports and approval requirements.

e. Gain reasonable assurance that CIDM is delivering on the benefits originally stated.

f. Gain reasonable assurance that stakeholder satisfaction is monitored.

g. Gain reasonable assurance that a benefit realization plan has been defined, approved and executed.

h. Gain reasonable assurance that the CIDM system executes the following key features effectively and efficiently:

    i. search function

    ii. version control

    iii. locking and unlocking documents

    iv. archiving material

    v. overall ease of use

Ensure performance attributes are defined and that remote sites and regions are abiding by them.

Appendix B – Knowledge management criteria and research

For the purpose of this audit, the following definition of knowledge management (KM) was used:

> "Knowledge Management is the practice of selectively applying knowledge from previous experiences of decision making to current and future decision making activities with the express purpose of improving the organization's effectiveness."

CIDM is an important component of the Department's KM strategy, and is important for INAC for the following reasons:

- The Department is required by Treasury Board (TB) policy to maintain records;[16]
- Effective KM reduces loss of information due to:
    - Obsolescence of media and innovation (especially technology);
    - Change in format and standards for storage and retrieval;
    - Changes in business processes;
    - Retiring workforce ("baby boomers" effect);
    - Changes in the organization (people changing roles or positions); and
    - Changes in relationships whether they are between entire organizations or even individuals (relationship capital or customer capital).
- CIDM provides a common workspace bridging ten provinces and three territories;
- CIDM provides high-quality record-keeping of informal messaging;
- CIDM provides access to information across the Department from anywhere with a network or phone connection; and
- CIDM helps to reduce paper workflow and usage.

Implementing effective knowledge management requires technology to be a key component of the framework. Knowledge repositories should include various forms of information, such as videos, audio files and graphics. We understand that CIDM has the capability to store information in these other formats, although they are outside the scope of the current system implementation.

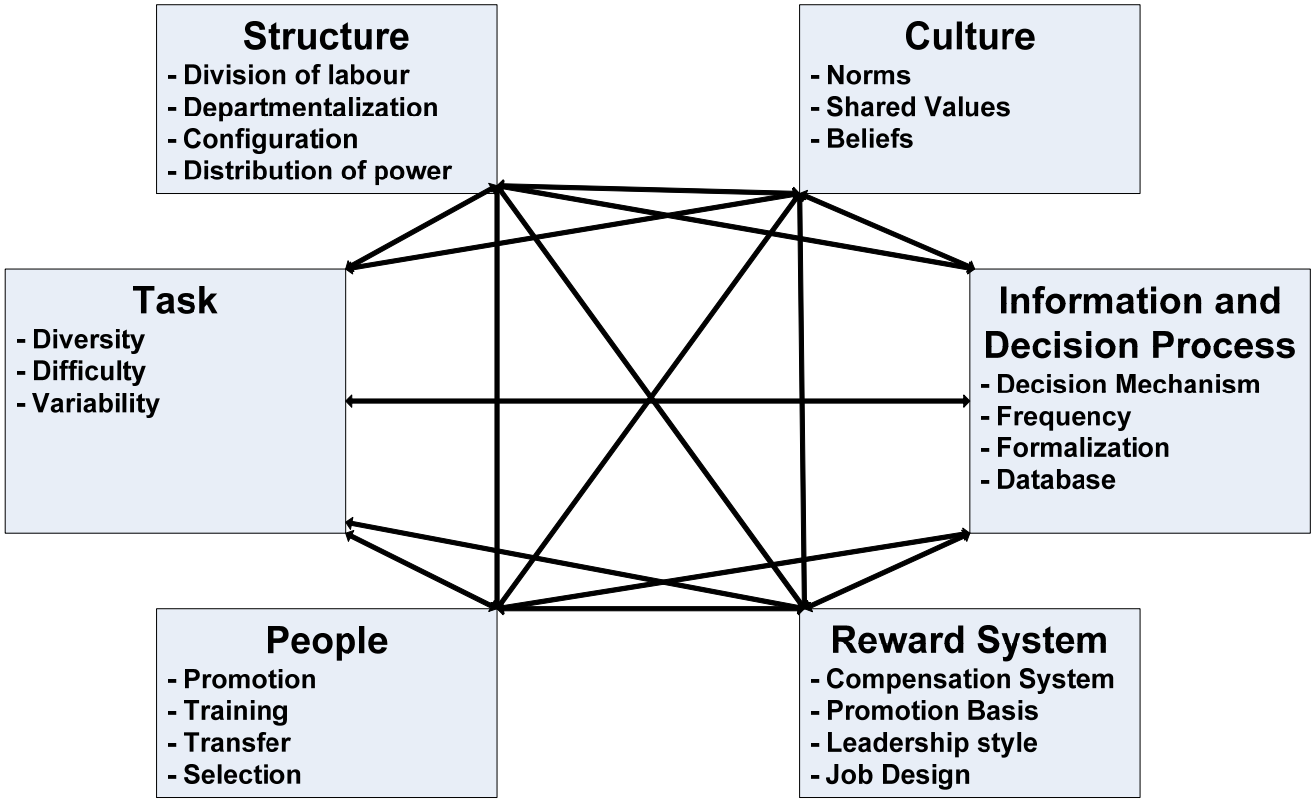
The goal of KM systems is to enhance four broad areas as follows:

- Increase productivity;
- Improve organizational responsiveness;

[16] "Policy on Information Management" Treasury Board of Canada Secretariat. 9 July 2009, Section 6.1.3. http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/gd-do/notes05-eng.asp.

- Improve organizational competency; and
- Stimulate and encourage innovation.

Effective KM allows organizations to be more productive and better able to respond to a dynamic business environment, and to improve competency in identifying and managing issues that are both operational and strategic in nature. In order to build effective KM systems that overcome inherent knowledge management challenges, the following organizational variables should be considered:



Research in knowledge management indicates that the following essential leading practices should be implemented to identify information to be retained: (Jennex, 2008)

- Use risk management techniques;
- Identify information which becomes important when aggregated; and
- Identify information supporting key management decisions.

According to research, "70% of organizations implementing an organization-wide strategy for knowledge transfer fails [sic] to realize improvement in performance or to develop core competencies". (Jennex, 2008) The low success rate is stated to be a result of the organizations' failure to do the following:

- Emphasize knowledge transfer as a business objective;

- Embed knowledge transfer in daily processes;
- Implement technology that facilitates the transfer of knowledge; and
- Foster a knowledge-sharing culture.

Other reasons for KM project failures include foregoing risk management techniques aimed at identifying critical information worth saving and collecting too much information, termed "data smog"[17] (Shenk, 1997). These factors should be considered when an information management solution such as CIDM is implemented in support of knowledge management.

[17] Shenk, D. (1997). *Data smog: Surviving the information glut.* HarperEdge Publishing.

Appendix C – Documents reviewed

CIDM Roles and Responsibilities

- CONSULTATION_GROUPS_FOR_POLICY_RENEWAL.DOC
- INFORMATION_STEWARDSHIP_GROUP_1ST_MEETING__BRIEFING_SESSION.DOC
- INFORMATION_STEWARDSHIP_GROUP_REPRESENTATIVES_-_MS_WORD_VERSION_OF_302467.DOC
- MANDATE_FOR_THE_INFORMATION_STEWARDSHIP_GROUP.DOC
- CIDM IT FRAMEWORK - MANUAL.doc
- DIRECTIVE_-_ELECTRONIC_DOCUMENT_MANAGEMENT_.DOC
- DIRECTIVE_-_ELECTRONIC_MAIL_(EMAIL)_MANAGEMENT_.DOC
- DIRECTIVE_-_IMAGING_OF_TEXT-BASED_BUSINESS_RECORDS.DOC
- DIRECTIVE_-_RECORD_KEEPING.DOC
- OVERVIEW OF THE RESPONSIBILITIES MATRIX RELATED TO FNITPCIDM DOCUMENT CAPTURE PROCESS.doc
- POLICY_-_INAC_INFORMATION_MANAGEMENT.DOC
- STANDARD - IM POLICY INSTRUMENT DEFINITIONS.doc
- WEBCIMS-CIDM ACCOUNTABILITY FRAMEWORK.doc
- DISCUSSION PAPER - STANDARD FNITP ROLEPERMISSION FOR REGIONAL IM STAFF USE.doc

Procurements/Agreements:

- CIDM SERVICE LEVEL AGREEMENT (SLA) AS DRAFTED BY ED PECK & CHRIS CLINE (JPG).jpg
- IM IT SERVICE LEVEL AGREEMENTS CFO WORKSHOP DISCUSSION SEPTEMBER 2008.ppt
- IT SERVICES SERVICE LEVEL AGREEMENT - NCR HQ.doc
- RDIM(CIDM)SLA.pdf
- SERVICE LEVEL AGREEMENT - ENTERPRISE IM - ELECTRONIC INFORMATION SUPPORT SYSTEMS.doc
- RDIMS SLA (SERVICE LEVEL AGREEMENT) A0416-07-4405 FOR SUPPORT 2007 2008.doc

CIDM Strategic Documentation:

- 2006 NATIONAL IM WORKSHOP ISSUE LOG REGIONAL PROFILING METADATA FOR TRANSFER PAYMENTS DOCUMENTATION .xls
- 2006 NATIONAL IM WORKSHOP REGIONAL PROFILING METADATA FOR TRANSFER PAYMENTS DOCUMENTATION IN CIDM.xls
- ARCHIVE OF CIDM5 METADATA STDS COLLABORATION PROJECT.zip
- CIDM 5 PROFILE FORM AND METADATA.mlm
- CIMD PROJECT PROFILE - CIDMFNITP - METADATA CONVENTIONS AND STANDARDS.doc
- DISCUSSION PAPER - METADATA - INFORMATION RETRIEVAL AND KNOWLEDGE MANAGEMENT MS WORD VERSION OF 33466.doc
- FNITP PTPNI - CIDM METADATA AUTOMATION MAPPING BY RECEPTION SUB-FUNCTION.xls
- GOVERNMENT OF CANADA RECORDS MANAGEMENT METADATA STANDARD.doc
- GUIDELINE - CIDM PROFILING PROTOCOLS AND BEST PRACTICES.doc
- IM WORKSHOP NOTES - METADATA.doc
- IMPLEMENTATION ISSUES (RDIMS METADATA).mlm
- MEETING RECORD - CIDM PROFILING METADATA CONVENTIONS - 2005-08-31.wpd
- METADATA CONVENTIONS AND STANDARDS FOR FNITPCIDM (APPLICATIONS LIBRARY).xls
- METADATA STANDARDIZATION DISCUSSION PAPER - MS WORD VERSION.doc

- METADATA STANDARDIZATION DISCUSSION PAPER.wpd
- MINUTES THESAURUS METADATA AT INAC.doc
- PROFILE REGIONAL METADATA AS OF AUG 5.xls
- PROFILE SCREEN METADATA FIELD DESCRIPTIONS.wpd
- SURVEY OF METADATA ELEMENTS IN CIDM, INTERNET, INTRANET AT INAC.wpd
- CRYSTAL REPORT - CIMD DOCUMENTS COMPARING PROFILE METADATA AGAINST SECURITY AND FILE NUMBER.xls
- PROCEDURE - REMOVING THE CONTENT OF PROTECTED C OR ABOVE DOCUMENTS PREVIOUSLY STORED IN CIDM.doc
- PROCEDURE - SAVING PROTECTED C AND ABOVE DOCUMENTS IN CIDM.doc
- CIDM5 UPGRADE - CHANGE REQUEST 747 - BAND AND TRIBAL COUNCIL RAW DATA.xls
- EIH CHANGE REQUEST TRACKING .xls
- EIRM CHANGE REQUEST - 30789 - HQ RECORDS OFFICE STAFF REQUIRE INCREASED ACCESS RIGHTS TO CIDM DOCUMENTS IN THE NCR AND IM LIBRARIES.doc
- EIRM CHANGE REQUEST - PROCESS DIAGRAM.vsd
- EIRM CHANGE REQUEST 20351 CIDM STANDARD FNITP ROLEPERMISSION FOR REGIONAL IM STAFF USE.doc
- EIRM CHANGE REQUEST 739761 SUMMARY LOG SHEET739761.xls
- EIRM CHANGE REQUEST TEMPLATE.doc
- EIRM CHANGE REQUEST30065 TO CREATE A NEW CIDM FIELD FOR THE INTEGRATION OF ETD.doc

Prioritized list of Information Security policies adhered to in design of CIDM:

- CIDM IT FORUM COMMUNICATION STRATEGY.doc
- CIDM5 UPGRADE COMMUNICATIONS.xls
- COMMUNICATION - CIDM CBT - INAC EXPRESS .doc
- COMMUNICATION - PLAN - IM AWARENESS.doc
- EIM COMMUNICATIONS PLAN 2005-2006 - MS WORD VERSION OF 383225.doc
- EIRM COMMUNICATIONS AND CHANGE MANAGEMENT PLAN 2005-2006.doc
- EIRM COMMUNICATIONS 2005 FALL 8TH ANNUAL IM WORKSHOP EVALUATION REPORT.doc
- INFORMATION NOTE - COMMUNICATIONS STRATEGY FOR CLIENTS CURRENTLY NOT USING CIDM 3 - MS WORD VERSION OF 305249.doc
- INFORMATION NOTE - STRATEGY FOR INACTIVE ACCOUNTS FOR CIDM UPGRADE IN HQ - MS WORD VERSION OF 306461.doc
- NCR-_151627-v1-COHERENT_IT_OPERATIONS_PRESENTATION_-_DIRECTORS_OF_CORPORATE_SERVICES.ppt
- NCR-%23218202-v1-CIDM_RENEWAL_PROPOSAL_-_KEY_ISSUES_-_PRESENTED_TO_RIMS_OCT_2003.pdf
- NCR-%23219459-v1A-DCS_PRESENTATION_ON_CIDM_RENEWAL_PROJECT.pdf
- BRIEFING NOTE - STRATEGY FOR INAC CENTRALIZED CIDM LIBRARY - 2006-06.doc
- CIDM IN THE CORPORATE INFORMATION STRATEGY VISION - MS WORD VERSION OF 46209.doc
- CIDM RENEWAL PROJECT PLAN REVIEW ASSESSMENT.doc
- CIDM RENEWAL PROJECT PROPOSAL MS WORD VERSION OF 184984 - SOME CORRUPTION.doc
- CIDM STORAGE MANAGEMENT STRATEGY.ppt
- CIMD 2008-2009 IM PLANNING SUMMARY DOCUMENT.xls
- CIMD PROJECT PROFILE - CIDM RENEWAL - STRATEGY DEFINITION FOR CIDM CENTRAL LIBRARY.doc
- CIMD PROJECT PROFILE - COLLABORATION, WEBCIMS, CIDM TRAINING SUPPORT.wpd
- CIMD STRATEGIC & OPERATIONAL PROJECTS - 2007-2008 .xls

- DISCUSSION PAPER - INFORMATION HANDLING PROTOCOLS FOR MIGRATION TO ELECTRONIC RECORD FOR CASE FILE TRANSFER PAYMENT DOCUMENTATION.doc
- DISCUSSION PAPER - LEGAL CONSIDERATIONS FOR MOVING TO ELECTRONIC RECORDS - MS WORD VERSION OF 369749.doc
- E-RECORD CHANGE MANAGEMENT PLAN FOR TP CASE FILE.doc
- EIRM IMIT PLANNING 2009 - 2012.xls
- EIRM ROADMAP 2007-2008 THROUGH 2009-2010.doc
- EIRM ROADMAP 2008-09 THROUGH 2010-2011.doc
- EIRMEIH ROADMAP 200809 TO 20102011.doc
- IM @ INAC BEING INFORMED - CIDM WORKOUT SUMMARY OF FINDINGS.wpd
- INFORMATION NOTE - STRATEGY FOR INACTIVE ACCOUNTS FOR CIDM UPGRADE IN HQ - MS WORD VERSION OF 306461.doc
- NCR-_180954-v1-CIDM_INITIATIVE_-_THE_WAY_AHEAD.ppt
- PROPOSAL FOR ESTABLISHING ELECTRONIC DOCUMENTS AS RECORDS.doc
- SINGLE LIBRARY HIGH LEVEL OVERVIEW FOR INAC.doc
- CIDM IMPLEMENTATION- WBS-COMMUNICATION BRANCH[1].mpp
- CIDM 5 HQ - PROJECT CLOSURE REPORT.wpd
- CIDM IT PROJECT PLAN 08-09[1].mpp
- CIDM RENEWAL PROJECT CONSOLIDATED PROJECT WBS[1].mpp
- CIDM5 UPGRADE NCR LIBRARY EIM PROJECT CLOSURE REPORT.wpd
- CITO CONSOLIDATED PROGRAM CHARTER.wpd
- CITO INTEGRATED SCHEDULE[1].mpp
- EIM CIDM UPGRADE PROJECT WBS 2003 - 2005[1].mpp
- EIM STRATEGIC IM INITIATIVES WBS.mpp
- EIRM PROGRAMPROJECT ASSIGNMENT MATRIX.xls
- EIRM PROJECT STATUS REPORT TRACKING 2007-2007.xls
- ICMS-CIDM INTEGRATION PROJECT WBS.mpp
- PR038 EIM WBS DEFINITION OF SERVICE LEVEL AGREEMENTS AND OPERATIONAL LEVEL AGREEMENTS.mpp
- PROJECT CHARTER - AUTOMATED CAPTURE OF FAXES IN FNITP CIDM PROJECT.doc
- WBS - DEVELOPMENT OF A DISPOSITION PROCESS FOR PAPER AND ELECTRONIC RECORDS.mpp
- WBS-CIDM UPGRADE- IOGC.mpp
- WBS FOR CIDM DEPLOYMENT METHODOLOGY.mpp
- WORK PLAN - DEFINE STRATEGY FOR INAC CONSOLIDATED CIDM LIBRARY.doc
- WORK PLAN - STRATEGY FOR CLEANUP CIDM AND COLLABORATION.mpp

CIDM Specifics:

- ADDITIONAL NOTES FOR CIDM BUSINESS CASE.doc
- BUSINESS CASE FOR DOSSIER INTEGRATION WITH CIDM.wpd
- CIDM BUSINESS CASE wpd
- CIDM RENEWAL PROJECT OVERVIEW OF POTENTIAL RETURN ON INVESTMENT.ppt
- AUDIT AND EVALUATION SECTOR INTERNAL BUSINESS RULES.doc
- BUSINESS RULES - RECORDKEEPING PROGRAM FOR TRANSFER PAYMENTS.doc
- CIDM & RECORDS MANAGEMENT BUSINESS RULES- INFORMATION MANAGEMENT UNIT - SEPRO.doc
- CIDM BUSINESS RULES - EXTRACTION OF DISCUSSIONS FROM COLLABORATION - 2006[1].03.07.doc
- CIDM BUSINESS RULES.doc

- CIDM BUSINESS RULES_V9[1].WPD
- INTERNAL CIDM BUSINESS RULES & PROCEDURES.doc
- LEARNING AND DEVELOPMENT DIRECTORATE - CIDM BUSINESS RULES.doc
- LMRB CIDM BUSINESS RULES.wpd
- MANITOBA REGION BUSINESS RULES AND PRACTICES.wpd
- REVIEW OF BC BUSINESS RULES.wpd
- SEPRO-CIDM BUSINESS RULES.wpd
- APPLICATIONS INTEGRATED WITH CIDM.doc
- CIDM 4 FEATURES OVERVIEW FOR STEERING COMMITTEE PRESENTATION.ppt
- CIDM APPLICATION EVOLUTION 2008 TO 2011.ppt
- CIDM ARCHITECTURE DIAGRAMS - WORD FORMAT.doc
- DISCUSSION PAPER INTEGRATION OF RM WITH THE INTEGRATED SCANNING SOLUTION.doc
- FRAMEWORK - CIDM INTERFACE PRINCIPLES.doc
- FUNCTIONAL REQUIREMENTS BACKGROUND OCR FOR APPLICATIONS LIBRARY.doc
- NCR-_229156-v1-SCOPE_DIAGRAM_FOR_CIDM.ppt
- TRIGGERS AND PROCEDURES FOR CIDM AT INAC.doc
- CIDM NAMING CONVENTIONS .xls
- CIDM PROFILING CONVENTION - INFORMATION MANAGEMENT BRANCH.xls
- GUIDE - CIDM PROFILING CONVENTIONS - IMB.xls
- CIDM RENEWAL PROJECT STEERING COMMITTEE ISSUES PRESENTATION 9 JANUARY 2004.ppt
- NCR-#222306-v2-CIDM_SEMINAR_PRESENTATION_-_2003-10-20.pdf
- PRESENTATION ON CIDM DEPLOYMENT METHODOLOGY.ppt

Training:

- PROCEDURE - ADDING A CIDM DOCUMENT TO WEBCIMS.doc
- PROCEDURE - MS PROJECT - INSERTING THE CIDM DOCUMENT NUMBER AND FILE NAME.doc
- PROCEDURE - MS WORD - INSERTING THE CIDM DOCUMENT NUMBER AND FILE NAME.doc
- PROCEDURE - WORKING WITH THE MAIL MERGE FUNCTION OF MS WORD DOCUMENTS STORED IN CIDM.doc
- ADVISORY INPUT ON MANDATORY CIDM TRAINING .mlm
- ALBERTA REGION CONTRIBUTION TO CIDM TRAINING CURRICULUM AND PRACTICES - AB REGION.mlm
- BC INPUT TO TRAINING ON CIDM.doc
- EDMONTON-_138927-V3-CIDM_END_USER_TRAINING_SESSION_OUTLNE[1].DOC.doc
- EDMONTON-_289724-V5-CIDM_5_END_USER_TRAINING_LESSON_PLAN[1].DOC.doc
- EDMONTON-_293924-V1-CIDM_5_ENDU_USER_TRAINING_PLAN__SHORT_VERSION[1].DOC.doc
- IM EDUCATION - PRODUCT 2 - COMPUTER BASED TRAINING ON CIDM.doc
- SASKATCHEWAN INPUT - REGINA-_64723-V1-CIDM_-_TRAINING_-_CIDM5_END_USER_CURRICULUM[1].DOC.doc
- SASKATCHEWAN INPUT - REGINA-_65422-V1-CIDM_-_TRAINING_-_CIDM5_ENDUSER_TRAINING_EVALUATION[1].WPD.wpd
- SASKATCHEWAN INPUT - REGINA-_103150-V1-CIDM_-_TRAINING_-_OVERVIEW_PRESENTATION[1].PPT.ppt
- SASKATCHEWAN INPUT - REGINA-_115365-V1-CIDM_-_TRAINING_-_AWARENESS_INFORMATION_PRESENTATION_STRIPPED_VERSION[1].PPT.ppt
- CBT WEB PAGE.doc
- CIDM TRAINING - ACTUAL IMAGE OF THE INTRANET WEBPAGE.doc
- QUICK REFERENCE GUIDE - CIDM.doc

- QUICK REFERENCE GUIDE - WEBTOP.doc
- STANDARD - CIDM END USER TRAINING CURRICULUM.doc
- TRAINING MANUAL - CIDM - END USER.doc
- TRAINING MANUAL - WEBTOP .doc

Project Expectations:

- CFO METRICS - 2009-01-19.xls
- CFO METRICS ANALYSIS 2009-01-19.xls
- DRAFT - PROJECT CLOSURE REPORT - INFORMATION MANAGEMENT BUSINESS ANALYSIS - SASKATCHEWAN.doc
- ISSUE COMPILATION - INFORMATION MANAGEMENT BUSINESS ANALYSIS - SASKATCHEWAN .doc
- PROJECT CHARTER - INFORMATION MANAGEMENT BUSINESS ANALYSIS - SASKATCHEWAN.doc
- PROJECT PLAN - INFORMATION MANAGEMENT BUSINESS ANALYSIS - SASKATCHEWAN - APRIL 2008.mpp
- RECOMMENDATIONS - INFORMATION MANAGEMENT BUSINESS ANALYSIS - SASKATCHEWAN.xls
- SURVEY - SK REGION IM ASSESSMENT ROUND TWO - QUALITATIVE DATA.doc
- VISIT REPORT - INFORMATION MANAGEMENT BUSINESS ANALYSIS - SASKATCHEWAN.doc
- CIDM METRICS - CIDM BUSINESS RULES.xls
- CIDM REGIONAL METRICS - Q1 (2005-2006).xls
- CIDM REGIONAL METRICS - Q2 (2005-2006).xls
- CRYSTAL REPORT - CIMD DOCUMENTS COMPARING PROFILE METADATA AGAINST SECURITY AND FILE NUMBER.xls
- IM SCORECARD MEASUREMENT METRICS.xls
- INAC IM METRICS ANALYSIS FOR Q2 PERIOD OF FY 2005-2006.doc
- REPORT - METRICS - INTEGRATED PERFORMANCE AND CORPORATE SYSTEMS .xls
- SCORE CARD METRICS - INFORMATION MANAGEMENT BRANCH IMB.xls

Operating and Maintenance Costs (yearly):

- ANALYSIS AND COSTING OF INFORMATION TECHNOLOGY OUTPUTS 20062007 (JOHN MURRAY REPORT).doc
- COSTS ASSOCIATED WITH THE MAINTENANCE OF CIDM 20092010.doc

Risk Assessment:

- THREAT RISK ASSESSMENT WORKSHOP REPORT - CIDM SOLUTION.rtf

Follow-up Questions (June 2009):

- 0 - CIDM AUDIT IM-IT QUESTIONS.doc
- 1. INAC Network Topology.jpg
- 2.a. CIDM Document Count and User Count per Region.XLS
- 2.b. Hardware Specifications for CIDM Server Environment.DOC
- 2.d. STANDARD - CIDM CONFIGURATION FOR E-RECORD.doc
- 7.a. CIDM RENEWAL PROJECT STEERING COMMITTEE ISSUES PRESENTATION 9 JANUARY 2004.ppt
- 7.a. PROCEDURE - HOW TO ADJUST CIDM ACCESS CONTROLS TO SHARE DOCUMENTS.doc
- 7.b. GUIDELINE - CIDM PROFILING PROTOCOLS AND BEST PRACTICES.doc
- 7.b. STANDARD - PROFILING CONVENTIONS FOR TRANSFER PAYMENT CASE FILES STORED IN REGIONAL CIDM.doc
- 7.d. FRAMEWORK - CIDM INTERFACE PRINCIPLES.doc
- 9. Info Security - 2009-2010 CRYSTAL REPORTS PROTECTED C AND ABOVE.pdf
- 9. PROCEDURE - REMOVING THE CONTENT OF PROTECTED C OR ABOVE DOCUMENTS PREVIOUSLY STORED IN CIDM.doc

- 9. PROCEDURE - SAVING PROTECTED C AND ABOVE DOCUMENTS IN CIDM.doc
- 15.c. STANDARD - ELECTRONIC DOCUMENTS AS BUSINESS RECORDS (E-RECORD).doc
- 18. CIDM RENEWAL PROJECT OVERVIEW OF POTENTIAL RETURN ON INVESTMENT.ppt
- 18. PRESENTATION - RIA CITO IMPLEMENTATION.ppt
- 15.b. IM Policy Instruments (Intranet)
    - Guidelines on mail management.PDF
    - CIDM 5/WebCIMS User Guide.PDF
    - Information management (IM) and information technology (IT) governance policy.PDF
    - INAC IM/IT Project Initiation and Approval Process.PDF
    - Policy on the management of records in support of program devolution.PDF
    - IM Policy Instruments.DOC
    - Procedures - How to use the Search module in WebCIMS.PDF

Atlantic Region Documentation:

- DRAFT_CIDM_BUSINESS_RULES_AND_PROCEDURES_FOR_THE_ATLANTIC_REGION.DOC
- ATLANTIC_REGIONAL_DIRECTIVE_FOR_COMPREHENSIVE_INTEGRATED_DOCUMENT_MANAGEMENT_(BUSINESS_RULES).DOC
- DIRECTIVE_-_COMPREHENSIVE_INTEGRATED_DOCUMENT_MANAGEMENT_-_CIDM_-_BUSINESS_RULES.DOC
- CIDM_5_END_USER_TRAINING.DOC
- CIDM_5_UPGRADE_TRAINING.DOC
- CIDM_5_QUICK_REFERENCE_GUIDE.DOC
- Information Management Scorecards – Executive Summary
- Information Management Scorecards – Analysis of Findings
- Information Management Scorecards – Senior Management Committee Presentation
- Information Management Scorecards – Action Plan
- Information Management Scorecards – Progress Report

Works Cited

Jennex, M. E. (2008). *Current Issues in Knowledge Management.* Hershey, PA: Information Science Reference.

Shenk, D. (1997). *Data smog: Surviving the information glut.* HarperEdge Publishing.