Audit of Corporate Information Management

Corporate Internal Audit Division (CIAD),
NSERC/SSHRC
March 31, 2011

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Background

The agencies[1] support scholarly endeavors in Canada's post-secondary institutions. More specifically, the Natural Sciences and Engineering Research Council of Canada (NSERC) supports post-secondary students in their advanced studies, promotes and supports discovery research, and fosters innovation by encouraging Canadian companies to participate and invest in post-secondary research projects in the natural sciences and engineering. The Social Sciences and Humanities Research Council of Canada (SSHRC) promotes and supports research and training in the humanities and social sciences. SSHRC also partners with public- and private-sector organizations to focus research, and aid the development of better policies and practices in key areas of Canada's social, cultural and economic life. NSERC and SSHRC are departmental agencies of the Government of Canada and report to Parliament through the Minister of Industry.

The Information Management Services (IMS) section, which is housed within the Information Management and Technology Services (IMTS) Division of the Common Administrative Services Directorate (CASD), is responsible for supporting the management of information, as a critical asset, throughout its life cycle. It provides advice and guidance to clients (NSERC and SSHRC) on all matters related to information management, with the purpose of enabling the agencies to meet their respective legislative and policy requirements.

Why it is important

The management of information is an essential element of effective management across Government of Canada (GoC) departments and agencies. Integrating information management considerations into all aspects of GoC business enables information to be used and recognized as a valuable asset. Furthermore, it enhances planning and decision-making processes by having information that is specific to business issues accessible, organized, timely and consistent across the organization. The Treasury Board Secretariat (TBS) *Policy on Information Management* (2007) recognizes this importance and requires departments and agencies to have an "efficient and effective information management to support program and service delivery; foster informed decision making; facilitate accountability, transparency, and collaboration; and preserve and ensure access to information and records for the benefit of present and future generations."

Audit objective

[1] For simplicity's sake, *agencies* is used throughout the report to refer to the Natural Sciences and Engineering Research Council of Canada (NSERC) and the Social Sciences and Humanities Research Council of Canada (SSHRC).

The objective of this audit was to examine the extent to which the agencies demonstrate regard for compliance with legislative requirements for information management;[2] and for efficiency[3] through the application of governance, training and awareness.

Key audit findings

A. Regard for compliance

1. Efforts have been made by the agencies to determine their current level of compliance with information management (IM) policy and legislation, but compliance was never measured. There was limited evidence that the agencies conducted agency-wide compliance assessments or reviews to understand if current processes and practices comply with GoC legislative and policy requirements.
2. The agencies have not conducted adequate assessments and evaluations to understand the business value and safeguarding requirements of its information holdings.

B. Regard for efficiency: governance

3. The clarity of the roles and responsibilities of the IM/information technology (IT) Bi-Council Steering Committee needs improvement. It's also unclear how these are communicated within the agencies.
4. Since the inception of the IM/IT Bi-Council Steering Committee, limited time was devoted to IM issues at the Committee meetings. When IM-related matters were raised, it was found that decisions and actions were not systematically identified and tracked to ensure appropriate and timely follow up by delegated "owners."

C. Regard for efficiency: training and awareness

5. Some good training and awareness initiatives have been implemented by the agencies. Many IM tools and information are available to all employees on the agencies' intranet pages.
6. Further improvements are needed in the following areas:
    a. the agencies lack an internal policy on IM that is geared to the needs of the agencies, and supported by a documented, corporate-wide suite of internal IM guidelines and directives to ensure information is managed efficiently; and
    b. an IM communications strategy has not been developed to inform staff of available training, tools and their policy and legislative requirements.

Conclusion

[2] **Definition of "compliance":** the development and maintenance of policy to ensure effective management of GoC information assets, assessment of departmental IM capacity, and monitoring of departmental compliance to policy (Treasury Board of Canada Secretariat).
[3] **Definition of "efficiency":** the minimum resource inputs to achieve a given quantity and quality of output (*2004 OAG Performance Auditing Manual*, Appendix A, Definitions).

The management of information is an essential function to enable the fulfillment of the agencies' mandate to fund Canadian research, partnerships and innovation. The audit found that the agencies had many good initiatives underway; however, these were often left in draft and/or were not communicated. Key elements required to facilitate compliance were found to be absent and, as such, the agencies' level of compliance is unknown. As for efficiency, the audit noted that the roles and responsibilities of the IM/IT Bi-Council Steering Committee should be clarified and that the agencies should provide additional direction to staff (i.e., internal policy on IM, guidelines, directives, etc.) to promote the efficient management of information. A robust IM framework/strategy needs to be implemented to ensure IM is standardized, and that practices and processes reduce delays in retrieval, minimize errors and protect against vulnerabilities.

1. BACKGROUND

The agencies support scholarly endeavors in Canada's post-secondary institutions. More specifically, the Natural Sciences and Engineering Research Council of Canada (NSERC) supports post-secondary students in their advanced studies, promotes and supports discovery research, and fosters innovation by encouraging Canadian companies to participate and invest in post-secondary research projects in the natural sciences and engineering. The Social Sciences and Humanities Research Council of Canada (SSHRC) promotes and supports research and training in the humanities and social sciences. SSHRC also partners with public- and private-sector organizations to focus research and aid the development of better policies and practices in key areas of Canada's social, cultural and economic life. NSERC and SSHRC are departmental agencies of the Government of Canada and report to Parliament through the Minister of Industry.

Not unlike many other government departments and agencies, NSERC and SSHRC manage a large volume of information that includes both electronic and physical (i.e., paper) information. The information holdings within the agencies can be categorized into two main groups: namely "program information" and "corporate information." Program information, which makes up the majority of paper records, includes all information relating to the administration of a program—such as applications, peer reviews, funding decisions and personal information (i.e., date of birth, address, Social Insurance Number etc.). Corporate information, on the other hand, is predominantly in electronic format and includes internally generated information—such as budgetary documents, briefs, correspondences, committee minutes, internal reports, memoranda, etc.

The TBS *Policy on Information Management* requires that Deputy Heads ensure "electronic systems are the preferred means of creating, using, and managing information." As such, the agencies have begun implementing an Electronic Documents and Records Management System (EDRMS) with an objective to create a consistent structure for organizing and retrieving information across the agencies. The selected EDRMS solution allows for the centralized management of corporate and program information, in both electronic and paper formats. This project employs a "phased-in" approach and is currently in the first implementation phase at NSERC and SSHRC.

The Information Management Services (IMS) section, which is housed within the Information Management and Technology Services (IMTS) Division of the Common Administrative Services Directorate (CASD), is responsible for supporting the management of information as a critical asset throughout its life cycle. The IMS section provides advice and guidance to clients on all matters related to information management, with the purpose of enabling the agencies to meet their respective legislative and policy requirements as per the TBS's policy on information management. This section, lead by a Chief of IM, is divided into three main areas: Information, Mail and Imaging and the EDRMS. The section has approximately 25 full-time positions and a budget of approximately $2.2 million (2010-11 fiscal year).

2. AUDIT OBJECTIVE AND SCOPE

The objective of this audit was to examine the extent to which the agencies demonstrate regard for compliance with legislative requirements for information management;[4] and for efficiency[5] through the application of governance, training and awareness.

The scope of the audit covered the following strategic areas of IM:

1. Regard for compliance
2. Regard for efficiency: governance
3. Regard for efficiency: training and awareness

The audit work was conducted over a six-month period between April and September 2010, using Corporate Internal Audit Division (CIAD) resources combined with the services of Deloitte during the planning phase. The review focussed on information available between January 2007 and September 2010.

3. AUDIT METHODOLOGY

The CIAD used the following methodology to conduct its work:

- File and document review of various sources of information—including committee meeting minutes, previous audits, planning documentation, project plans, policies, guidelines, training material, etc.
- Conduct interviews with key stakeholders—such as IM employees, EDRMS project team, program directors, and senior management—on major issues, challenges and risks related to IM
- Conduct interviews with IM Life Cycle partners, including Library and Archives Canada, and TBS

The audit was carried out and completed using standards set by the Institute of Internal Auditors (IIA). The criteria (Appendix I) were based on various TBS IM policies and directives, including the TBS *Policy on Information Management* and the TBS *Directive on Recordkeeping*. The conclusions were drawn based on the assessment of audit findings against these criteria.

4. KEY AUDIT FINDINGS

A. Regard for Compliance

Compliance typically consists of two areas: how well an organization follows its own rules (internal compliance), and how well an organization follows the rules imposed on it by outside groups (external compliance). Both are important and can impose restrictions on a business.

Information Management activities in all departments and agencies are directed by several GoC legislations, policies and directives. The key IM legislative and policy documents that NSERC and SSHRC must use to manage their program and corporate

[4] **Definition of "compliance":** the development and maintenance of policy to ensure effective management of GoC information assets, assessment of departmental IM capacity, and monitoring of departmental compliance to policy (*Treasury Board of Canada Secretariat*).
[5] **Definition of "efficiency":** the minimum resource inputs to achieve a given quantity and quality of output (*2004 OAG Performance Auditing Manual*, Appendix A, Definitions).

information are outlined in Appendix II. The purpose of these documents is to ensure that information is managed in a manner that the GoC deems to be prudent, efficient and respectful of security and privacy matters.

4.1 The level of compliance with GoC legislation and policy requirements is unknown.

One of the first steps in determining the level of compliance is to identify exactly where gaps exist. The audit found that the agencies have not engaged in an exercise to determine their current level of compliance with IM legislation and policy requirements. More specifically, there was limited evidence that the agencies conducted compliance assessments or reviews to understand if current processes and practices comply with the GoC legislative and policy requirements. In the absence of a review, the agencies have little information concerning their current level of compliance, and what actions are needed to ensure mandatory requirements are met. While the agencies have embarked on many good IM-related initiatives, it is very difficult to implement best practices that have long-term viability without first knowing whether gaps in compliance exist.

4.2 Assessments to identify business value of information holdings were limited.

The TBS *Directive on Recordkeeping* requires that departments identify the "information resources of business value, based on an analysis of departmental functions and activities, carried out by a department to enable or support its legislated mandate." One of many ways to identify business value is to conduct Threat and Risk Assessments (TRAs) or Business Impact Analyses (BIAs). These types of analyses not only assist management in understanding their critical holdings, but also identify the inherent risks (i.e., security, privacy, loss, etc.) and articulate recommendations to ensure the safeguarding and integrity of this information within an organization.

The audit found that the agencies have not conducted adequate work to understand the business value and safeguarding requirements of their information holdings. Over the years, the agencies have adopted a decentralized model where each division is responsible for managing its own information. The audit noted that there is no central functional authority to oversee the collection and analysis of information assessments; therefore, the agencies' ability to appropriately protect valuable information assets could be compromised.

Recommendations:

1. The agencies should conduct an IM compliance assessment to identify the current level of compliance with IM policy and legislation. This should include actions needed to ensure all mandatory requirements are met.
2. The agencies should conduct formal agency-wide analyses of key information holdings to determine the business value and the appropriate level of protection needed.
3. The agencies should identify a central functional authority to oversee the collection and analysis of information assessments.

B. Regard for Efficiency: Governance

Corporate governance refers to the process and structure for overseeing the direction and management of an organization so that it carries out its mandate and objectives effectively.[6] Efficient governance is dependent on the establishment of effective oversight bodies, communicated committee mandates that clearly define roles with respect to governance, and clearly defined and communicated strategic direction, and objectives aligned with these mandates.[7]

As previously mentioned, both agencies share a common IMS section that is responsible for the provision of IM policy and strategic guidance on the management of information to senior management and staff. To provide oversight, in 2006 the agencies created the IM/IT Bi-Council Steering Committee (IM/IT Bi-Council) which is composed of vice-president-level representatives, and is responsible for providing IM/IT strategic direction, planning advice, expertise on policy development, and approvals of major projects. Since its inception, the Committee was chaired by the Vice-President of CASD and, in the summer of 2010, it was decided that the Committee be chaired by the Executive Vice-Presidents of SSHRC and NSERC on an annual, rotational basis.

The IM/IT Bi-Council's Terms of Reference limit the Committee's decision-making responsibilities to approvals of IM/IT strategic plans and major IM/IT projects. SSHRC's strategic decisions and approvals are made by the Senior Management Committee (SMC), based on recommendations and suggestions from the Operational Management Committee (OMC). Similarly, NSERC's strategic decisions and approvals are made by the President's Management Committee (PMC), based on recommendations and suggestions from the Executive Management Committee (EMC).

4.3 The position of the IM/IT Bi-Council Steering Committee within the agencies' governance structure needs to be clarified and clearly documented.

The linkages between the IM/IT Bi-Council and the agencies' other management committees have not been clearly documented to allow for a clear understanding of reporting channels, approval processes, or overall communications requirements for IM projects, policies or issues. The lack of clarity has led to inconsistent understanding of committee roles and responsibilities in regards to IM. Despite efforts made within the IMS section to document processes and develop strategies, the approval process continued to be a challenge and resulted in many key documents remaining in draft.

The recent internal IM policy approval exercise demonstrates the lack of clarity with regards to the agencies' decision-making process. In January 2008, draft internal IM policies were tabled at IM/IT Bi-Council for approval. Since approving internal policies was not part of IM/IT Bi-Council's mandate, it was decided that the internal policies be presented to the OMC and the EMC for approval. In January 2010, the same draft internal IM policies were tabled at OMC and the committee recommended that the TBS *Policy on Information Management* be adopted instead of finalizing internal IM policies. Subsequently, at the July 2010 meeting, the IM/IT Bi-Council agreed with OMC's recommendation, and the TBS *Policy on Information Management* was adopted for both NSERC and SSHRC. This item was never presented or discussed at EMC, or at either

[6] Office of the Auditor General of Canada, December 2000.
[7] *Core Management Controls: A Guide for Internal Auditors*, Treasury Board of Canada, November 2007.

of the agencies' decision-making bodies—SMC and PMC. Without clearly defined linkages between IM/IT Bi-Council and the agencies' other committees, there is potential for both bypassing the decision-making process, and for confusion with respect to committee mandates when dealing with IM issues.

Currently, there is an audit of internal governance underway at SSHRC, and this will provide a perspective on internal governance. Recognizing this, the recommendation for this finding would be more appropriately addressed holistically in the Internal Governance Audit report. Once this SSHRC Internal Governance Audit is completed, NSERC can review the recommendations to identify if principles are applicable to its own internal governance and subsequently address issues, where appropriate.

4.4 Limited time devoted to IM issues at IM/IT Bi-Council Steering Committee meetings.

The audit noted that apart from the topic of the EDRMS project itself, IM-related discussions at the IM/IT Bi-Council meetings were limited. Between 2007 and 2010, the Committee concentrated on various IT matters, with a large amount of time spent on addressing the now-defunct Enterprise Awards Management System (EAMS). When IM-related matters were raised, it was found that decisions and actions were not systematically identified and tracked to ensure appropriate and timely follow up by delegated "owners."

For example, a draft IMTS strategic plan was created in 2007 (covering the 2007-10 timeframe) and it was presented at the October 2007 IM/IT Bi-Council meeting. This draft strategy included a long list of IT strategies and a number of IM-related actions, initiatives and projects to be implemented during the defined period. Discussions at this meeting noted that the plan was very IT-centric and did not consider enough client requirements or incorporate IM components. It was unclear what decision was made at the time, but this document was never officially approved by any of the agencies' management committees. Without an approved IMTS strategic plan, the agencies cannot be assured that IM projects and initiatives are aligned with the strategic direction of the agencies.

Recommendations:

4. The IM/IT Bi-Council should clarify its roles and responsibilities and communicate them to the agencies.
5. The IM/IT Bi-Council should ensure that IM issues are adequately discussed and monitored.

C. Regard for Efficiency: Training and Awareness

Data and information are critical organizational assets and are a resource that should be considered as valuable as employees, buildings and products. Data stewardship and the governance of information assets are essential parts of any relevant information systems strategy for the 21st century. Although the IMS section has a key role to play in the management of information, all employees within the agencies are responsible and must manage information in ways that meet this requirement.

The importance of employees' responsibilities and awareness of IM practices is outlined in the TBS *Policy on Information Management* which emphasizes that, "all employees are responsible for applying information management principles, standards, and practices as expressed in Treasury Board and departmental frameworks, policies, directives, and guidelines in the performance of their duties, and for documenting their activities and decisions."

To fulfill this requirement, the agencies have developed the IM Awareness On-line Course that aims to enhance employees' IM awareness level. This on-line module replaced an in-class IM training course and has been available to employees since the fall of 2009. It offers a high level overview of IM—including major legislative requirements, roles and responsibilities, and current IM Life Cycle practices. Employees are expected to access and complete this module as part of the EDRMS project rollout, although completion is not mandatory.

4.5 Some good training and awareness initiatives have been implemented.

In addition to the IM Awareness On-line Course, the IMS section has posted IM tools that are available to all employees on the NSERC and SSHRC intranet sites. These include:

- *Naming Documents in the Corporate Shared Drive*
- *Managing Information of Departing Employees*
- *Information Classification, Categorization and Marking Guide for Security Purposes*
- *Standards for Secure Handling of Information*
- *To Delete or Not to Delete*
- *How to Request Information from the Information Management Services (IMS)*
- *Storage and Disposal Form*

To supplement these initiatives, the agencies' intranet pages also provide links to relevant GoC documentation, such as IM policy and legislative documents.

Furthermore, the agencies have taken steps to ensure that the competencies of IM employees are current. IMS section employees have completed the Personal Learning Center (PLC) Certification Program in Records Management Fundamentals from the University of Toronto to ensure that IMS section employees are well versed in IM.

4.6 Further improvements are needed to ensure a robust IM training and awareness program.

The existing training and awareness provided by the IMS section consists of one training session called the IM Awareness On-line Course. This serves as a broad, baseline IM awareness training tool that provides a general overview of policy and legislative requirements. The IMS section also provides training to employees as EDRMS is implemented in each division. This one-day session informs employees on how to manage their corporate electronic records and documents in the EDRMS tool. While these sessions and available tools on the intranets are a good start, the audit noted a few critical areas where further improvements are needed.

4.6.1 The agencies lack an internal IM policy supported by a corporate-wide suite of key guidelines and directives to ensure information is managed efficiently.

Appendix III describes the seven key stages of an IM life cycle that are necessary for efficient information management. This life cycle describes "what" needs to be done, but "how" to complete these stages is left to each individual department/agency to develop. In other words, departments/agencies are expected to develop their key directives and guidelines tailored to their own needs. The audit found that direction provided to employees explaining "how" to manage information through each stage of the IM life cycle is often provided verbally by IM analysts. Additionally, in some cases, employees manage their information using a "common-sense" approach. With limited documented agency-wide internal guidelines to operationalize high-level GoC legislative and policy requirements, the agencies do not have assurance that information assets will be managed accurately, consistently and efficiently.

The audit further noted that, in some cases, divisions have taken it upon themselves to incorporate elements of IM requirements into their own documented processes. It can be argued that this approach is superior because the processes to manage IM are then tailored to the needs of each division. However, the time and duplication of effort by each division devoted to developing, communicating and training employees on these processes can be eliminated by having a centralized function that coordinates the development of an agency-wide suite of guidelines. This would, in turn, reduce duplication of effort, improve standardization and enhance consistency. These tools can help guide employees to manage information in ways that align with GoC IM requirements.

4.6.2 An IM communications strategy has not been developed to inform staff of available training and tools, and their legislative and policy requirements.

One key requirement of the 2009 TBS *Directive on Recordkeeping* is that key methodologies, mechanisms and tools to support the departmental recordkeeping requirements throughout the IM life cycle be established and implemented. Although training and tools are available to address this requirement, such as the IM Awareness On-line Course, the agencies have not developed an IM communications strategy to ensure that employees are aware of the training and tools available.

In 2001, an *Audit of Recorded Information Management* completed by Nashel Management Inc. identified this same issue and recommended the development of a communications strategy. The 2001 audit also recommended that periodic IM information sessions be conducted and regular communications to employees occur. The management response agreed to these recommendations at the time, however there is limited evidence that these recommendations have been implemented. Without a comprehensive communications strategy, the agencies have limited assurance that employees are made aware of the available IM tools that intend to facilitate efficiency. The agencies also lack assurance that all pertinent policy and legislation will be communicated to staff. The lack of communication has a potential impact on the agencies' ability to not only manage information more efficiently, but also to ensure compliance with legislation and policy requirements.

Recommendations:

6. The agencies should consider developing a common IM policy that is geared towards the needs of the agencies, and support this policy with an agency-wide suite of internal guidelines and directives.
7. The agencies should develop an IM communications strategy to inform staff of available training and tools, and their legislative and policy requirements. This will help the agencies' ability to not only manage information more efficiently, but also to ensure compliance with legislation and policy requirements.

5. CONCLUSION

The management of information is an essential function to enable the fulfillment of NSERC and SSHRC's mandates. The audit found that the agencies had many good initiatives underway but that these were often left in draft and/or were not communicated. Key elements required to facilitate compliance were found to be absent, and as such, the agencies' level of compliance is unknown. As for efficiency, the audit noted that the IM/IT Bi-Council Steering Committee mandate needs to be clarified and communicated. Moving forward, a robust IM strategy and framework needs to be in place to enhance retrieval, minimize errors and protect against loss or vulnerabilities.

6. MANAGEMENT RESPONSE TO AUDIT RECOMMENDATIONS

ITEM	RECOMMENDATION	ACTION PLAN	TARGET DATE
1	The agencies should conduct an IM compliance assessment to identify the current level of compliance with IM policy and legislation. This should include actions needed to ensure all mandatory requirements are met.	The IMS section last conducted an IM assessment in 2006. Since that time, the IM policy framework for the GoC has been completely renewed, and new legislation introduced (e.g., *Federal Accountability Act*). It is agreed that an updated compliance assessment is required at this time. To address this recommendation, the IMS section will: 1) conduct an IM compliance assessment to identify the current IM policy and legislation requirements and commitments; evaluate the agencies effectiveness in compliance; and define an action plan for priority items and area of improvement. The IM compliance assessment shall follow the recommended methodology and framework prepared for Library and Archives Canada and TBS. The IM compliance assessment action plan should be evaluated and updated every three to four years at a minimum; and 2) revise and update the IM strategy for the agencies, to address the priorities and areas for improvement identified in the IM compliance assessment, with a multi-year action plan.	Q2 – 2011/12 Q4 – 2011/12

2	The agencies should conduct formal agency-wide analyses of key information holdings to determine the business value and the appropriate level of protection needed.	There are many, disparate information holdings across the agencies. Since January 2009, the IMS section has undertaken a phased implementation strategy to identify and consolidate these silos of information into an authoritative corporate repository—the EDRMS. The IMS section is currently in the process of completing the EDRMS implementation to all staff in both agencies. The first phase of the EDRMS implementation addresses the requirements for managing the unstructured electronic information of the agencies, permitting the effective management of electronic documents and e-mails of "business value", as well as the management of physical (i.e., paper) records. The implementation of EDRMS in each division of the agencies includes an analysis of the network shared drives holdings and an IM needs assessment. This assessment identifies the key business information on the client's shared drive, a consistent filing structure for managing information in EDRMS, and appropriate access controls and file classifications for protecting and preserving that information. While EDRMS addresses the unstructured information (i.e., e-mails and electronic documents) up to the level of Protected B, it does not address the effective management and protection of: • sensitive information that is Protected C, Confidential or Secret; • structured information holdings in corporate applications such as HRIS or FPAM;	Q2 – 2011/12

		• the case files and "workflow" of applications for grants (i.e., funding opportunities); • documents and collaboration with peer review committees and institutions through the corporate extranets (i.e., Sharepoint); and • Web content that is published to the intranets and external (i.e., public) Web sites of the agencies. To address these additional information holdings, the IMS section shall: 1) conduct an assessment of the case files for applications and grants to identify a Standard for electronic records (eRecord) of applications. This assessment will identify the key information products (i.e., records of business value) that are produced through this process, and will define standards for managing and protecting this information in electronic format; and 2) conduct a Statement of Sensitivity (SOS) of all of the information management holdings across the agencies. The SOS shall identify the key collections or holdings, the level of sensitivity and business value of the information, and the key controls required to protect or manage that information. The SOS should be conducted in coordination with the IMTS strategy, to ensure that it incorporates existing and planned systems.	Q1 – 2011/12 Q4 – 2011/12

3	The agencies should identify a central functional authority to oversee the collection and analysis of information assessments.	The Executive Director of the IMTS section is the functional authority within the agencies to oversee the collection and analysis of information assessments. To address the recommendation, the IMTS section will: 1. clarify its role for the collection and analysis of information assessments and the role of the IM/IT Bi-Council. Roles and responsibilities will be defined as the internal governance structure and terms of reference of the IM/IT Bi-Council; 2. develop and launch an agency-wide IM communications strategy to inform staff of the IM framework (including a suite of policies, directives, guidelines and best practices); and 3. develop an IM assessment process, where each new IM/IT system and existing core business services, are evaluated (in conjunction with an SOS and TRA) to determine the key information products (i.e., inputs, templates, and outputs) that need to be managed by the system or service, and the lifecycle requirements of each type of information. In accordance with the *Directive on Recordkeeping*, the IM assessment shall identify and document the risk profile of each information resource, taking into consideration legal and regulatory risks, access to information, security of information and the protection of personal information requirements.	Q1 – 2011/12 Q4 – 2011/12 Q4 – 2011/12

4	The IM/IT Bi-Council should clarify its roles and responsibilities and communicate them to the agencies.	The IMS section will: 1. work with IM/IT Bi-Council to review and implement an IM governance structure; and 2. help identify the IM roles and responsibilities for the internal governance structure	Q1 – 2011/12
5	The IM/IT Bi-Council should ensure that IM issues are adequately discussed and monitored.	1. Information Management (and other IM/IT policies) will be a standard agenda item at the IM/IT Bi-Council. 2. The IM compliance assessment action plan will be evaluated and updated every three to four years at a minimum and shall be tabled and approved by the IM/IT Bi-Council. 3. Annual monitoring and review of issues: the IMS section will produce an IM annual report, measuring and reporting on outcomes, initiatives, statistics and key services. This annual report will be prepared in conjunction with, and in support of, the annual Management Accountability Framework reporting requirements, and shall monitor the progress on the IM compliance assessment action plan. The annual report should be tabled and approved by the IM/IT Bi-Council.	Q1 – 2011/12 Q3 – 2011/12 Q4 – 2011/12
6	The agencies should consider developing a common IM policy that is geared towards the needs of the agencies, and support this policy with an agency-wide	The IMS section agrees that a common IM policy (including a suite of directives, standards, guidelines and best practices), needs to be developed and adopted.	

	suite of internal guidelines and directives.	In April 2009, an implementation strategy and concept of operations were developed by the IMS section, to identify an effective IM accountability framework and a road map to implement this framework and an EDRMS. The IMS section has been in the process of implementing many of these elements of the IM framework in parallel to the EDRMS project. The following actions will address the recommendation and formalize an agency-wide IM framework: 1. Complete an IM "micro-site" on the Intranet, providing self-paced training resources, guidelines and best practices for end-users; 2. Develop a common IM Policy (including a suite of directives, standards, guidelines and best practices), geared towards the needs of the agencies. The IM policy will be presented to the OMC, EMC and IM/IT Bi-Council for approval. 3. The IMS section will develop and launch an agency-wide IM communications strategy to inform staff of the IM framework (including a suite of policies, directives, guidelines and best practices).	Q1 – 2011/12 Q3 – 2011/12 Q4 – 2011/12
7	The agencies should develop an IM communications strategy to inform staff of available training and tools, and their legislative and policy requirements. This will help the agencies' ability to not only manage information more efficiently, but	For the past two years, IM communications has been delivered almost solely through the implementation process of the EDRMS project. A renewed IM Awareness On-line Course, guidelines and best practices and new tools are being delivered to each existing employee of the agencies, as EDRMS is implemented in their divisions.	

	also to ensure compliance with legislation and policy requirements.	As the initial implementation of EDRMS is completed, the IMS section will need to implement additional tools and processes to ensure effective ongoing communication and IM support. The actions cited in Recommendation 6 will address this.	

APPENDIX I – Audit Criteria and Sources

Audit Criteria	Sources
1) The agencies use clearly defined governance to report on and make strategic decisions regarding IM matters.	TBS *Policy on Information Management* TBS *Directive on Recordkeeping* TBS *Directive on Information Management Roles and Responsibilities* TBS *Policy on Government Security*
2) The agencies provide IM training and awareness to ensure that information is managed with regard for policy and legislative requirements.	TBS *Directive on Recordkeeping* TBS *Policy on Privacy Protection*
3) The agencies have developed and implemented IM policies to ensure that information is managed in accordance with GoC legislative requirements and TBS policies.	*Privacy Act* *Access to Information Act* TBS *Policy on Privacy Protection* TBS *Policy on Government Security* TBS *Directive on Recordkeeping* TBS *Directive on Privacy Impact Assessment*
4) The agencies manage information through the IM lifecycle with regard for efficiency.	TBS *Policy on Information Management* TBS *Directive on Recordkeeping* TBS *Directive on Information Management Roles and Responsibilities* *Privacy Act* *Library and Archives Canada Act*

APPENDIX II – Key Legislative and Policy Documents

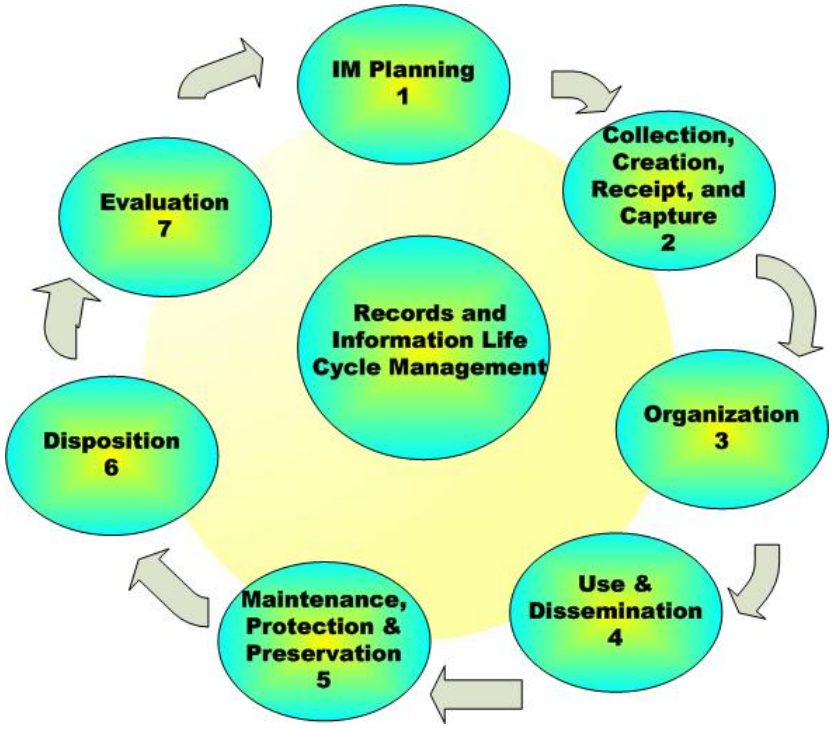
- TBS *Policy on Information Management*
  This policy took effect on July 1, 2007. The objective of this policy is to achieve efficient and effective information management to support program and service delivery; foster informed decision-making; facilitate accountability, transparency, and collaboration; and preserve and ensure access to information and records for the benefit of present and future generations.

- TBS *Directive on Information Management Roles and Responsibilities*
  This directive took effect on October 8, 2007. The objective of this directive is to identify the roles and responsibilities of all departmental employees in supporting the deputy head in the effective management of information in their department.

- TBS *Directive on Recordkeeping*
  This directive took effect on June 1, 2009. The objective of this directive is to ensure effective recordkeeping practices that enable departments to create, acquire, capture, manage and protect the integrity of information resources of business value in the delivery of Government of Canada programs and services.

- Other relevant policies, directives and acts are:
  - the TBS *Policy on Government Security*;
  - the TBS *Directive on Privacy Impact Assessment*;
  - the TBS *Policy on Privacy Protection*;
  - *Privacy Act*;
  - *Access to Information Act*; and
  - *Library and Archives of Canada Act*.

APPENDIX III – Records and Information Life Cycle Management[8]



- **Stage 1: IM Planning**
  Learn how early IM planning integrates records and IM perspectives into your daily activities, setting the stage for easier and more effective practices.

- **Stage 2: Collection, Creation, Receipt and Capture**
  To support effective IM, many important issues need to be addressed when new information assets are created.

- **Stage 3: Organization**
  Making the right assets available by properly organizing them is critical to effectively finding and sharing information.

- **Stage 4: Use and Dissemination**
  Timely, accurate and available information assets are the result of smart practices when using and disseminating records and information.

- **Stage 5: Maintenance, Protection and Preservation**
  Records and information that are correctly maintained, protected and preserved remain useful and available now, and in the future.

[8] www.collectionscanada.gc.ca/government/products-services/007002-2012-e.html

- **Stage 6: Disposition**
  Disposition routines ensure the availability of still-useful records over time, avoid costly storage backlogs, and transfer historically significant records into archival care.

- **Stage 7: Evaluation**
  Your IM policies and practices will improve over time when you routinely evaluate their effectiveness.

Audit Team

Chief Audit Executive:	Phat Do
Lead Auditors:	Benjamin Cyr, Patricia Morrell
Auditors:	Alice Hanlon, John-Patrick Moore